Business Continuity Solutions

BUSINESS CONTINUITY | **SonicWALL CDP Series**

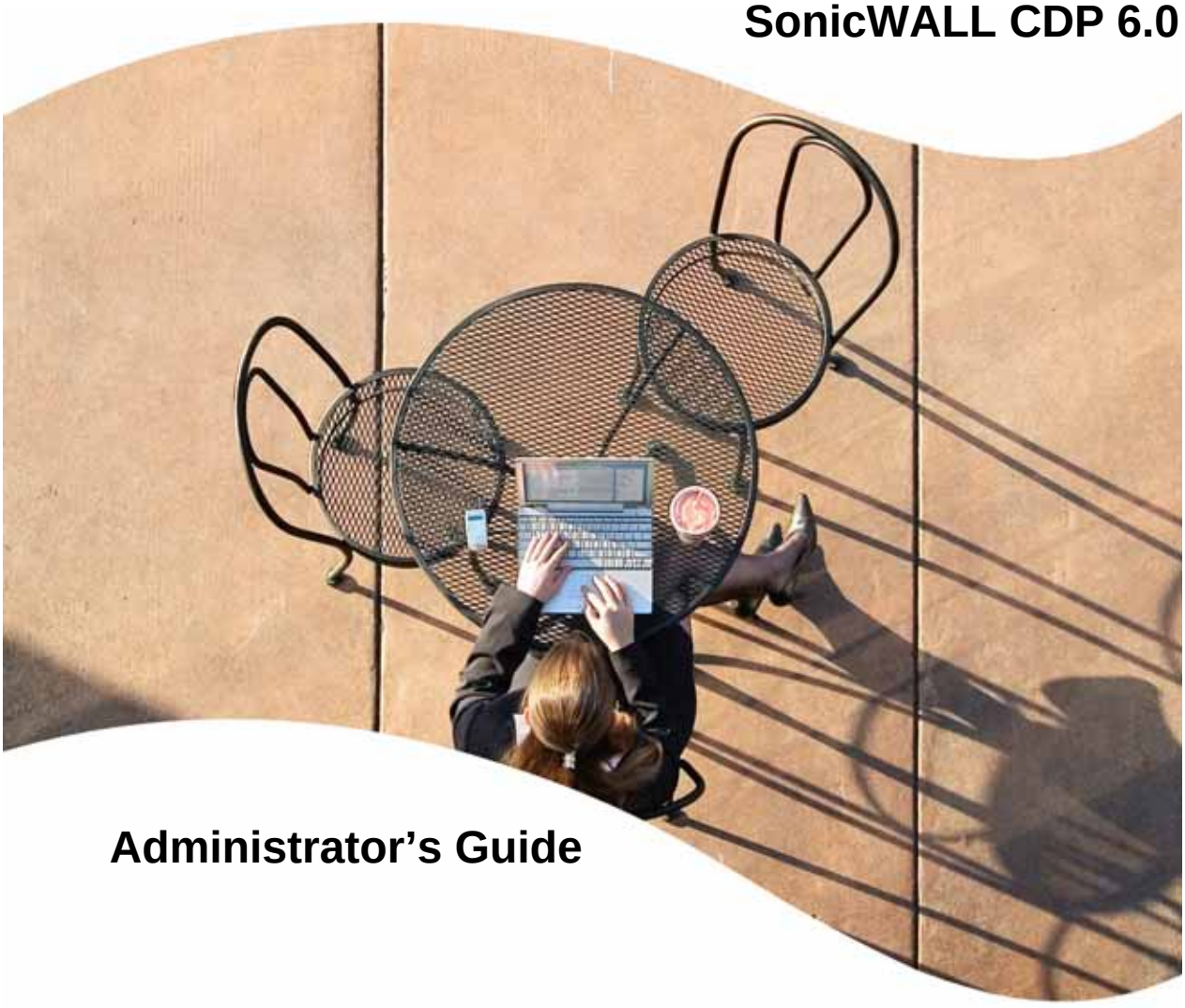
SonicWALL CDP 6.0
Administrator's Guide

SonicWALL CDP On-Demand Video:

http://www.demosondemand.com/clients/sonicwall/001/page/demos.asp#productdemos

SONICWALL®

SonicWALL CDP 6.0



Administrator's Guide

SonicWALL, Inc.
2001 Logic Drive
San Jose, CA 95124-3452
Phone: +1.408.745.9600
Fax: +1.408.745.9300
E-mail: info@sonicwall.com

Copyright Notice

© 2011 SonicWALL, Inc.

All rights reserved.

Under the copyright laws, this manual or the software described within, cannot be copied, in whole or part, without the written consent of the manufacturer, except in the normal use of the software to make a backup copy. The same proprietary and copyright notices must be affixed to any permitted copies as were affixed to the original. This exception does not allow copies to be made for others, whether or not sold, but all of the material purchased (with all backup copies) can be sold, given, or loaned to another person. Under the law, copying includes translating into another language or format.

Specifications and descriptions subject to change without notice.

Trademarks

SonicWALL is a registered trademark of SonicWALL, Inc.

Microsoft Windows XP, Windows Vista, Windows 7, Windows Server 2003, Windows Server 2008, Exchange 2003, Exchange 2007, Exchange 2010, SQL 2005, SQL 2008, Internet Explorer, SharePoint, and Active Directory are trademarks or registered trademarks of Microsoft Corporation.

Netscape is a registered trademark of Netscape Communications Corporation in the U.S. and other countries. Netscape Navigator and Netscape Communicator are also trademarks of Netscape Communications Corporation and may be registered outside the U.S.

Firefox is a trademark or registered trademark of the Mozilla Foundation.

Adobe, Acrobat, and Acrobat Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the U.S. and/or other countries.

Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

SonicWALL GPL Source Code

GNU General Public License (GPL)

SonicWALL will provide a machine-readable copy of the GPL open source on a CD. To obtain a complete machine-readable copy, please send your written request, along with a certified check or money order in the amount of US $25.00 payable to "SonicWALL, Inc." to:

General Public License Source Code Request
SonicWALL, Inc. Attn: Jennifer Anderson
2001 Logic Drive
San Jose, CA 95124-3452

Limited Warranty

SonicWALL, Inc. warrants that commencing from the delivery date to Customer (but in any case commencing not more than ninety (90) days after the original shipment by SonicWALL), and continuing for a period of twelve (12) months, that the product will be free from defects in materials and workmanship under normal use. This Limited Warranty is not transferable and applies only to the original end user of the product. SonicWALL and its suppliers' entire liability and Customer's sole and exclusive remedy under this limited warranty will be shipment of a replacement product. At SonicWALL's discretion the replacement product may be of equal or greater functionality and may be of either new or like-new quality. SonicWALL's obligations under this warranty are contingent upon the return of the defective product according to the terms of SonicWALL's then-current Support Services policies.

This warranty does not apply if the product has been subjected to abnormal electrical stress, damaged by accident, abuse, misuse or misapplication, or has been modified without the written permission of SonicWALL.

DISCLAIMER OF WARRANTY. EXCEPT AS SPECIFIED IN THIS WARRANTY, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, SATISFACTORY QUALITY OR ARISING FROM A COURSE OF DEALING, LAW, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE MAXIMUM EXTENT ALLOWED BY APPLICABLE LAW. TO THE EXTENT AN IMPLIED WARRANTY CANNOT BE EXCLUDED, SUCH WARRANTY IS LIMITED IN DURATION TO THE WARRANTY PERIOD. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, THE ABOVE LIMITATION MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION. This disclaimer and exclusion shall apply even if the express warranty set forth above fails of its essential purpose.

DISCLAIMER OF LIABILITY. SONICWALL'S SOLE LIABILITY IS THE SHIPMENT OF A REPLACEMENT PRODUCT AS DESCRIBED IN THE ABOVE LIMITED WARRANTY. IN NO EVENT SHALL SONICWALL OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION, LOSS OF INFORMATION, OR OTHER PECUNIARY LOSS ARISING OUT OF THE USE OR INABILITY TO USE THE PRODUCT, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY ARISING OUT OF THE USE OF OR INABILITY TO USE HARDWARE OR SOFTWARE EVEN IF SONICWALL OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event shall SonicWALL or its suppliers' liability to Customer, whether in contract, tort (including negligence), or otherwise, exceed the price paid by Customer. The foregoing limitations shall apply even if the above-stated warranty fails of its essential purpose. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATION OR EXCLUSION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

Guide Conventions

The following Conventions used in this guide are as follows:

Convention	Use
Bold	Highlights items you can select or that provide labels in the SonicWALL CDP Web Management Interface. Also highlights a value to enter into a field.
Italic	Highlights a book title or an item of special note.
Menu Item > Menu Item	Indicates a multiple step Management Interface menu choice. For example, **Security Services > Content Filter** means select **Security Services**, then select **Content Filter**.

Icons Used in this Manual

These special messages refer to noteworthy information, and can include a symbol for quick identification:

Tip — A timesaving tip.

Note — Important information on a feature that requires callout for special attention.

Cross Reference: Provides a pointer to related information in the Administrator's Guide or other resources.

SonicWALL Technical Support

For timely resolution of technical support questions, visit SonicWALL on the Internet at <*http://www.sonicwall.com/us/Support.html*>. Web-based resources are available to help you resolve most technical issues or contact SonicWALL Technical Support.

To contact SonicWALL telephone support, see the telephone numbers listed below:

North America Telephone Support

U.S./Canada - 888.777.1476 or +1 408.752.7819

International Telephone Support

Visit <*http://www.sonicwall.com/us/support/contact.html*> for the latest technical support telephone numbers.

More Information on SonicWALL Products

Contact SonicWALL, Inc. for information about SonicWALL products and services at:

Web: http://www.sonicwall.com
Email: sales@sonicwall.com
Phone: (408) 745-9600
Fax: (408) 745-9300

Current Documentation

Check the SonicWALL documentation Web site for that latest versions of this manual and all other SonicWALL product documentation.

http://www.sonicwall.com/us/Support.html

Table of Contents

Table of Contents

SonicWALL CDP Overview

What Is SonicWALL CDP? 2
Why Use SonicWALL CDP? 4
How Does SonicWALL CDP Work? 5
How the SonicWALL CDP Web Management Interface Works 6
How the SonicWALL CDP Appliance Works 9
How the SonicWALL CDP Agent Works 9
How Backup Policies Work 11
How Rules Work 15
How Scheduling Works 16
How Bare Metal Recovery Works 18
How the SonicWALL CDP Offsite Service Works 19
How SonicWALL CDP Local Archiving Works 20

Initializing the CDP Appliance

Supported Platforms and Deployment Requirements 21
System and Network Requirements 22
About the SonicWALL CDP Appliance 22
Requirements for Supported Applications 30
Microsoft Exchange 30
Microsoft Active Directory and System State 30
Microsoft SQL Server 30
Microsoft SharePoint 30
Registering the SonicWALL CDP Appliance 31
Registering the Appliance on MySonicWALL 31
Activating the SonicWALL CDP Appliance 33

Updating and Managing the SonicWALL CDP Appliance. 35
Checking Firmware and Software Updates 35
Storing the Offsite Service Encryption Key 35
Resetting a Lost Password 35

Configuring System Settings

System Interface Overview 38
Understanding the System Status 39
Understanding System RAID 40
Configuring the System Settings 42
Changing the Password 42
Configuring Time Settings 43
Configuring NTP Settings 44
Configuring Administrative Email Settings 45
Specifying Alerts 46
Configuring Reports Settings 47
Adding a SonicWALL CDP Appliance to GMS. 49
Configuring the Offsite Service. 52
Exporting or Importing Preferences 54
Administrative System Tasks and Settings 55
Restarting the Appliance 55
Upgrading Appliance Firmware 56
Purging Data from the SonicWALL CDP Appliance 56
Restoring Data from Offsite 57
Resetting to Factory Defaults 59
System Diagnostics 59
System Licenses and Registration 60
Registration Status. 60
Licenses 61
Manual Keyset. 61
System Activity Progress. 62

Configuring Network Settings

Network Interface Overview 63
Configuring Network Settings. 64
Configuring Appliance Host Name and Domain 64
Configuring IP, Subnet, and Gateway Addresses 65

Configuring the Domain Name Server Address 66
Testing Network Connectivity 66
Checking Network Settings 67
Tracing Network Routes 68
Testing URL Connectivity 69
Resolving URLs 70

Creating Files and Folders Backup Policies

Policy Interface Overview 72
Creating a Files and Folders Object 73
Creating a Schedule Object 75
Creating a Backup Task Object 79
About Trimming Algorithms 81
Creating a Global Policy 82

Managing Agents

Agents Interface 86
Managing Agents 87
Adding a New Agent Friendly Name 88
Editing an Agent’s Name 89
Resetting an Agent’s Key 90
Deleting an Agent 90
Selecting an Agent’s Policy 91
Browsing Agents Files 92
Viewing Agent Policy Summaries 94
About the Agent User Interface 94
Agent User Interface Overview 95
Using the Agent UI as Administrator 96
Creating and Managing Backup Policies 98

Bare Metal Recovery

About Bare Metal Recovery 99
Bare Metal Recovery Interface Overview 99
Configuring Bare Metal Recovery Accounts 100
Adding a Bare Metal Recovery Account 101
Editing a Bare Metal Recovery Account 101
Using Bare Metal Recovery 102

Viewing the Logs

Logs Interface Overview 103
Viewing the CDP Log 104
Viewing the Fileset Log 105
Viewing the Error Log 106

Configuring and Understanding Reports

Reports Interface Overview 108
Agent Summary Reports 109
Agent Summary Graph 109
Agent Summary Table 111
Disk Space by File Type Reports 112
Disk Space by File Type Chart 113
Disk Space by File Type Table 115
Disk Space Summary Reports 116
Graph 116
Table 116
Detailed Event List Reports 117
Table 117
Agent Events Summary Reports 119
Graph 119
Table 119
Daily Events Summary Reports 120
Graph 120
Table 120
Schedule Backup Reports 121
Graph 121
Configuring Scheduled Reports Delivered by Email 122

Backing Up Applications

Creating Schedules for Application Backups 124
Backing up Exchange 2010 126
Backing Up a User Mailbox 126
Backing Up InfoStore Databases 133
Backing up Exchange 2007/2003 139
Backing Up a User Mailbox 139
Backing Up a Storage Group 145

Backing Up SharePoint 151
Creating an Application Object for SharePoint 151
Scheduling Backups for SharePoint 152
Configuring a Backup Task for SharePoint 153
Verifying SharePoint Backup Activity 154
Backing up System State and Active Directory 156
Creating an Application Object for System State and Active Directory . . . 156
Scheduling Backups for System State and Active Directory 158
Configuring a Backup Task for System State 158
Verifying System State and Active Directory Backup Activity 159
Backing up Microsoft SQL Server 161
Adding a SQL Server Backup Application Object 162
Scheduling Backups for Microsoft SQL 163
Configuring a Backup Task for Microsoft SQL Database Backups 163
Verifying Microsoft SQL Backup Activity 164
SQL Authentication 167

Recovering Backed Up Data

Recovering Files and Folders 172
Recovering Data from an Offsite Appliance 174
Recovering Data from Microsoft Exchange 176
Recovering Exchange 2010 User Mailboxes 176
Recovering Exchange 2010 InfoStore 179
Recovering an Exchange 2007/2003 User Mailbox 181
Recovering an Exchange 2007/2003 Storage Group 184
Recovering SharePoint 189
Recovering System State and Active Directory 191
Restarting the Domain Controller in Safe Mode 191
Restoring Active Directory and System State 192
Recovering Data from Microsoft SQL Server 196
Recovering SQL Using the Agent User Interface 196
Additional Information 199

Configuring Site-to-Site Backup and Recovery

Site-to-Site Service Overview 201
What is the Site-to-Site Service? 202
Benefits of the Site-to-Site Service 202

How Does the Site-to-Site Service Work? 203
Preparing for the Site-to-Site Service 205
Site-to-Site Service Best Practices 205
Administrator Prerequisites 206
Purchasing Licenses and Support 206
Configuring the Downstream CDP Appliance 208
Configuring the Upstream CDP Appliance Quota 209
Removing a Downstream CDP 209
Selecting Files for Offsite Backup. 210
Viewing Backed Up Files on the Offsite Appliance 210
Recovering Data From the Upstream Appliance. 210
Deleting Data From the Upstream Appliance 212
Replacing the Downstream CDP Appliance 212
Disaster Recovery Using the Offsite Service 213

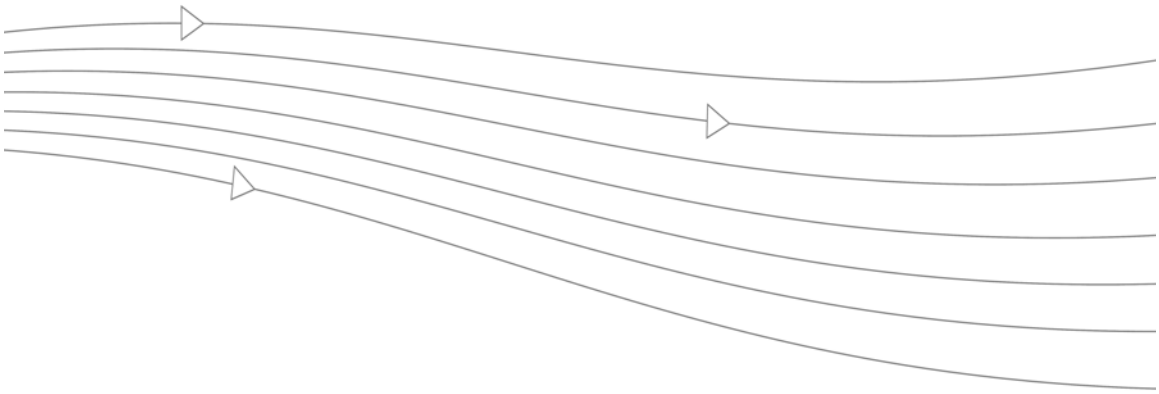
Using Local Archiving

SonicWALL CDP Local Archiving Overview 215
How Does Local Archiving Work? 216
Local Archiving Configuration Overview. 216
Prerequisites for Local Archiving 216
Creating a Local Archive 217
Verifying Local Archiving Success. 220
Ejecting the USB Device 220
Restoring Client Data from a Local Archive. 221
Restoring Server Applications from a Local Archive 223
Creating an Automatic Local Archive Task 226

Appendix 227

Help Overview. 228
Troubleshooting SonicWALL CDP 228
Appliance Troubleshooting 228
Software Troubleshooting 228
Backup and Recovery Troubleshooting. 229
Recovery when RAID Fails. 232
Configuring SonicOS Security Services for SonicWALL CDP 232
Clearing the Enforce Host Tag Search for CFS Setting 233
Setting up Security Services for SonicWALL CDP 233

Technical Frequently Asked Questions 235
Command Line Interface Reference 236
Glossary 248
Related Documents 250
User Guides 250
Contributors 250
Index



Chapter 1: SonicWALL CDP Overview

Protect your network using SonicWALL CDP (Continuous Data Protection), a secure backup solution that runs continuously, archiving file and application data from assigned agents (servers, laptops or PCs intended for backup using SonicWALL CDP).

SonicWALL CDP replicates data in real time, capturing new, changed and deleted information. By storing multiple versions of each file and application revision, SonicWALL CDP can recall data from nearly any point in time.

In the event of local disaster, data can be recovered from the secure SonicWALL CDP Offsite Service.The Offsite Service is an optional service that backs up your data at a North American or European site. For more routine data recovery needs, the SonicWALL CDP appliance provides instant, onsite data recall. SonicWALL CDP works even when users are on remote laptops connected by IPsec or SSL VPN connections.

SonicWALL CDP includes an appliance, a Web Management Interface, Agent User Interface, and Offsite Service.

This section contains the following subsections, which provide an introduction to the SonicWALL CDP features and benefits:

- "What Is SonicWALL CDP?" section on page 2
- "Why Use SonicWALL CDP?" section on page 4
- "How Does SonicWALL CDP Work?" section on page 5
  - "How the SonicWALL CDP Web Management Interface Works" section on page 6
  - "How the SonicWALL CDP Appliance Works" section on page 9
  - "How the SonicWALL CDP Agent Works" section on page 9
  - "How Bare Metal Recovery Works" section on page 18
  - "How the SonicWALL CDP Offsite Service Works" section on page 19
  - "How SonicWALL CDP Local Archiving Works" section on page 20

What Is SonicWALL CDP?

SonicWALL CDP protects your network from data loss. SonicWALL CDP is a disk-based data backup and recovery system that provides protection for assigned agents, regularly preserving the latest file versions and database revisions locally, and if configured, storing full folder and full database revisions to the secure Offsite Service.

Backups are performed regularly by SonicWALL CDP, ensuring that new versions of files or application revisions are continuously updated. In addition, older versions of each file are stored, allowing recovery from multiple points in time.

SonicWALL CDP includes the following components: The SonicWALL CDP Web Management Interface, Appliance, Offsite Service, Agent User Interface and Service, Local Archive Manager, and Bare Metal Recovery.

Each SonicWALL CDP component is described below.

- **SonicWALL CDP Web Management Interface**—The SonicWALL CDP Web Management Interface is a Web-based interface that provides the system administrator the ability to configure, create, and apply global policies and tasks for the SonicWALL CDP appliance. The Web Management Interface also provides initial system setting configuration for the SonicWALL CDP appliance, as well as system diagnostics, and allows for a full purge of data from the appliance. For detailed SonicWALL CDP management interface specifications, refer to the "How the SonicWALL CDP Web Management Interface Works" section on page 6.
- **SonicWALL CDP Appliance—**The SonicWALL CDP appliance is a dedicated disk backup appliance that collects data blocks from agents for storage and for secure transmission to the Offsite Service (if configured). For detailed SonicWALL CDP appliance specifications, refer to the "How the SonicWALL CDP Appliance Works" section on page 9 and the "About the SonicWALL CDP Appliance" section on page 22.
- **SonicWALL CDP Offsite Service**—The SonicWALL CDP Offsite Service is a subscription service that provides protection against local disasters including theft, power surges and server crashes. Full file revisions from the SonicWALL CDP appliance are securely transmitted to the Offsite Service and stored for emergency recovery. The Offsite Service can be configured to use a North American or European data center. For detailed SonicWALL CDP Offsite Service specifications, refer to the "How the SonicWALL CDP Offsite Service Works" section on page 19 and the "Site-to-Site Service Overview" section on page 201.
- **SonicWALL CDP Agent User Interface**—The SonicWALL CDP Agent User Interface software is installed on every agent (server, laptop or PC intended to be backed up on the SonicWALL CDP appliance), and provides individual users and system administrators the ability to configure, create, and apply local backup policies, and the ability to view backup status and recover lost data. User access privileges to the appliance using the Agent User Interface are configured by the SonicWALL CDP appliance administrator using the Web Management Interface. For more information about the SonicWALL CDP Agent User Interface specifications, refer to the "How the SonicWALL CDP Agent Works" section on page 9 and the "About the Agent User Interface" section on page 94. The *SonicWALL CDP Agent User's Guide* provides detailed information about using the Agent User Interface.
- **SonicWALL CDP Agent Service**—The SonicWALL CDP Agent Service software is installed automatically with the SonicWALL Agent User Interface. By running continuously in the background of each agent, the Agent Service enables backup of folders and application revisions as it performs handshaking with the appliance, transmits data, and listens for Windows Event Notifications. For detailed SonicWALL CDP Agent Service specifications, refer to the "How the SonicWALL CDP Agent Works" section on page 9 and the "About the Agent User Interface" section on page 94.

- **Local Archive Manager**—The Local Archive Manager is a separate application, installed on an agent machine, that allows an administrator to archive some or all of the contents of your SonicWALL CDP appliance onto a USB device. This feature can also be used to create a portable backup that can be restored at another site that does not have a SonicWALL CDP appliance. Data can be archived to the USB device in encrypted format. For more information about local archiving, see the "SonicWALL CDP Local Archiving Overview" section on page 215.
- **Bare Metal Recovery**—Bare Metal Recovery is a separate, standalone application, which provides the administrator with the option to create a hard disk image backup of information stored on a disk, including the operating system files, applications and configuration files, software updates, personal settings, documents, and other data. For detailed Bare Metal Recovery specifications, refer to the "How Bare Metal Recovery Works" section on page 18.

Why Use SonicWALL CDP?

SonicWALL CDP is a complete and reliable data protection solution that eliminates exposure to threats of data loss, using the same security technology implemented by major financial and government institutions.

Specifically developed for the business and remote office networks, SonicWALL CDP is employed in network environments with business requirements that necessitate continuous data backup. SonicWALL CDP also provides real-time, continuous data protection for laptops and remote agents connected by IPsec or SSL VPN.

Running seamlessly, SonicWALL CDP captures the most recent file and application revisions, maintaining multiple versions of each backed up file. SonicWALL CDP stores backed up data on a local SonicWALL CDP appliance for instant recovery, and if configured, to the secure SonicWALL CDP Offsite Service for protection against local disaster.

You control SonicWALL CDP, specifying which agents will use the appliance, selecting files and applications for automatic backup, and applying custom filters for non mission-critical file types.

SonicWALL CDP provides the following key features:

- **Continuous Data Protection**—SonicWALL CDP replicates data in real time, capturing new, changed and deleted information. SonicWALL CDP works even when users are on laptops or other remote connections using IPsec or SSL VPN.
- **Offsite Service**—SonicWALL CDP Offsite Service protects businesses against power surges, theft, server crashes and other disasters by backing up full files and full database revisions to a secure data center. The administrator can configure a bandwidth management schedule as well as adjust the synchronization interval so that backups are performed when network usage is at its lowest. You can select a North American or European data center during the appliance registration process.
- **Instant Recovery—**Because SonicWALL CDP utilizes an onsite appliance for data storage, agents have instant access to old file versions and can recover data at any time. And, agents have the ability to restore their own data without help from an IT administrator.
- **Multiple File Versions**—SonicWALL CDP saves multiple versions of every file, not just the latest version. Therefore, any user on the network can instantly retrieve a previous version of a document, even after they have saved over it. SonicWALL CDP allows recovery of data from multiple points in time.
- **Security**—Transmission of data to the SonicWALL CDP Offsite Service is secured by the same 256-bit AES (advanced encryption standard) and SSL (secure socket layer) encryption technologies implemented by major financial institutions and government agencies. SonicWALL CDP also utilizes public-key encryption and digital certificates as an additional layer of protection.
- **Intelligent Applications**—SonicWALL CDP integrates a collection of intelligent software applications. One such application is a backup reporting tool, which provides constant visual data backup verification. The tool places a highlighted SonicWALL stamp on each protected file so the user knows that the SonicWALL CDP is working.
- **Application Support**—SonicWALL CDP supports most business applications. Supported agent applications include Outlook and Outlook Express, and supported server applications include Microsoft Exchange, Active Directory and SQL Server.
- **RAID Support**—Some SonicWALL CDP appliances support RAID (redundant array of independent disks), providing additional failover protection in the event of a disk failure. The SonicWALL CDP 6080B, 6080, 5040B, and 5040 include RAID 5, block-level data striping with distributed parity across the drive set. The SonicWALL CDP 4440i also includes RAID 5. The SonicWALL CDP 3440i includes RAID 1, data mirroring from one drive onto another.

How Does SonicWALL CDP Work?

SonicWALL CDP replicates data in real time by storing multiple revisions of files and applications defined by policies and tasks set by the administrator and agents. Each element of the SonicWALL CDP works synchronously to ensure that data is protected continuously, in real time.

SonicWALL CDP includes the following major components:

- Web Management Interface
- Appliance
- Agent User Interface
- Agent Service
- Bare Metal Recovery
- Offsite Service
- Local Archiving

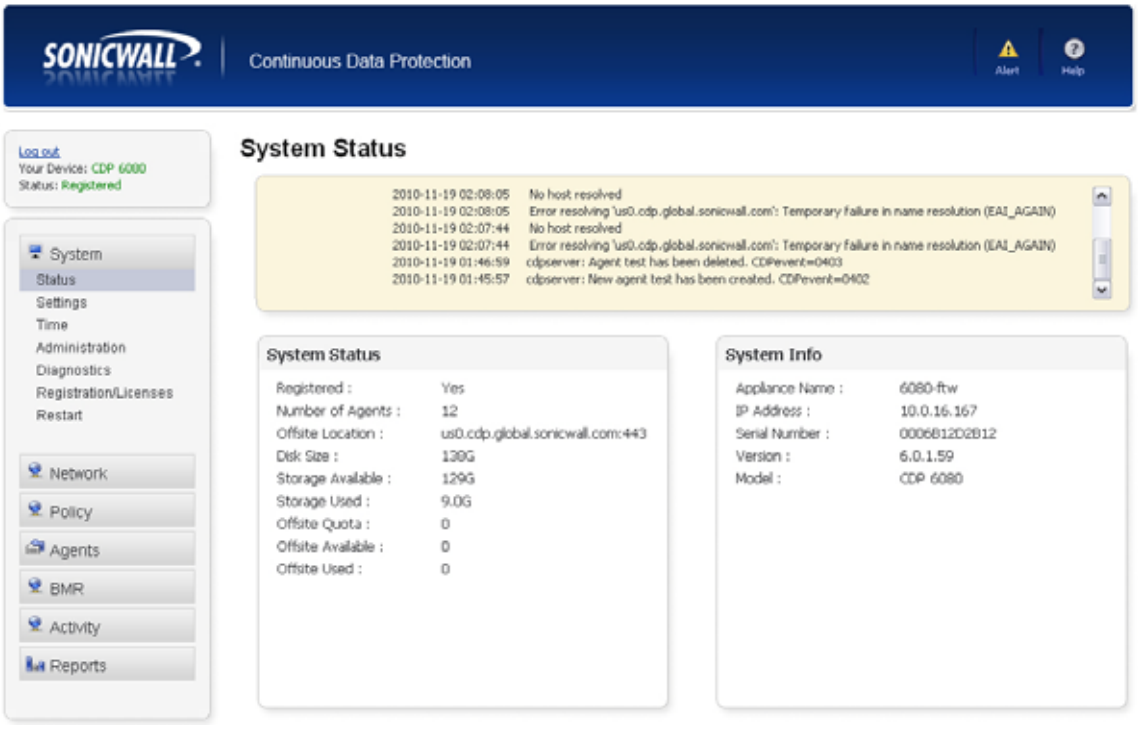
This section provides an overview of the SonicWALL CDP components and related topics. This section contains the following subsections:

- "How the SonicWALL CDP Web Management Interface Works" section on page 6
- "How the SonicWALL CDP Appliance Works" section on page 9
- "How the SonicWALL CDP Agent Works" section on page 9
- "How Backup Policies Work" section on page 11
- "How Rules Work" section on page 15
- "How Scheduling Works" section on page 16
- "How Bare Metal Recovery Works" section on page 18
- "How the SonicWALL CDP Offsite Service Works" section on page 19
- "How SonicWALL CDP Local Archiving Works" section on page 20

How the SonicWALL CDP Web Management Interface Works

The operating system inside the SonicWALL CDP appliance is called firmware. The **SonicWALL CDP Web Management Interface** is a Web-based interface that allows the SonicWALL CDP administrator to configure the SonicWALL CDP appliance firmware.

The **SonicWALL CDP Web Management Interface** is used by the SonicWALL CDP administrator to configure local and global policies, obtain logs and reports, set email notifications and other administrative settings, configure network settings, and manage agents.



Individual agents (workstations and servers) can connect to the SonicWALL CDP appliance and back up files and applications by running the SonicWALL CDP Agent software. Administrators can control the flow of data from the agents to the appliance(s) by using the SonicWALL CDP Web Management Interface to:

- Set local and global policies and tasks for agents
- Specify a maximum backup allotment (quota)
- Filter to include or omit specific file types

The Web Management Interface also allows the administrator to register the appliance, view and configure system and network settings, and purge data from the appliance.

After the initial set up of your SonicWALL CDP, which includes registering your SonicWALL CDP appliance on MySonicWALL, you must activate your appliance using the Web Management Interface. The Web Management Interface is used to insert the registration code or manual keyset that is obtained from MySonicWALL.

For more information about the registration and initial setup of your SonicWALL CDP appliance, refer to the *SonicWALL CDP Getting Started Guide* for your model.

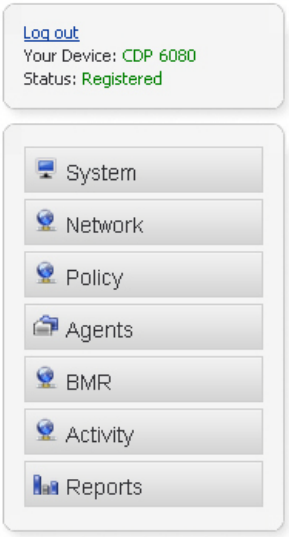
Alert and Help Options

The alert and help options are located in the header of the Web Management Interface.

Header	Description
Alert	Provides a shortcut to the Activity > Error Log.
Help	Provides a shortcut to view Online Help.

Navigation Overview

The navigation options are located in the left pane beneath the header.

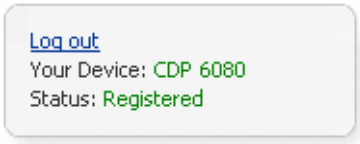


Two panels are visible:

- **Status Panel**: Displays the Log Out option and status of the administrator's appliance. This panel is located above the Navigation Menu.
- **Navigation Menu**: Allows the administrator to navigate the Web Management Interface.

Status Panel

The Status panel provides administrators with the login status, the name of the SonicWALL CDP appliance that the Web Management Interface is currently accessing, and the registration status of the accessed appliance.



Option	Description
Log Out	Logs the administrator out of the Web Management Interface.
Your Device	Lists the name of the device the administrator is logged into.
Status	Displays the current appliance registration status.

Navigation Menu

The Navigation Menu allows the administrator to navigate the appliance features.

Option	Description
System	Provides access to to view and configure system Status, Settings, Time, Administration, Diagnostics, Registration/ Licenses, and Restart. For more information, refer to "System Interface Overview" section on page 38.
Network	Provides access to to view and configure network Settings and Connectivity. For more information, refer to "Network Interface Overview" section on page 63.

Policy	Provides access to to view and configure Files and Folders, Schedules, Backup Tasks, and Policies. For more information, refer to “Policy Interface Overview” section on page 72.
Agents	Provides access to to view and configure Manage and Browse Agent Files. For more information, refer to “Managing Agents” section on page 87.
BMR	Provides access to to view and configure Bare Metal Recovery Accounts. For more information, refer to “About Bare Metal Recovery” section on page 99.
Activity	Provides access to to view the CDP Log, Fileset Log, and Error Log. For more information, refer to “Viewing the CDP Log” section on page 104.
Reports	Provides access to to view reports pertaining to the Agent Summary, Disk Space by File Type, Disk Space Summary, Detailed Event List, Agent Events Summary, Daily Events Summary, Schedule Backup, and reporting Configuration. For more information, refer to “Reports Interface Overview” section on page 108.

How the SonicWALL CDP Appliance Works

The **SonicWALL CDP appliance** performs three main tasks: Data processing, data storage, and if configured, data transmission to the Offsite Service.

The appliance receives data blocks from the Agent Service and compares them to existing blocks in order to discover new or modified information. The appliance stores the new or modified data blocks, and if configured, securely transmits them to the Offsite Service.

The appliance is connected, using a standard CAT5 or higher Ethernet cable, to your local area network (LAN). The SonicWALL CDP appliance requires configuration of a static IP address in order to communicate with your network, and an agent must be connected to the same LAN as the appliance to connect to it.

The SonicWALL CDP appliance communicates with the Web Management Interface, Agent Service, and, if configured, to the Offsite Service. The appliance communicates with the SonicWALL CDP Offsite Service for registration and storage using HTTPS (TCP 443), providing enhanced security and greater levels of compatibility with network perimeter devices. As a result, your network must be configured to allow HTTPS (TCP 443) communication.

To ensure that the appliance performs at its peak, it will automatically alert the administrator if it is close to reaching capacity. If the appliance is busy, or if an agent has become disconnected from the network, the agent will continue to attempt communication until a successful backup has been completed.

How the SonicWALL CDP Agent Works

The **SonicWALL CDP Agent User Interface** and **Agent Service** are installed at the same time. The Agent Service runs continuously in the background as a service, allowing backups of files, folders, and application revisions.

The Agent User Interface is a graphical user interface that allows users to control agent backup to and recovery from the SonicWALL CDP appliance. User access privileges to the appliance using the Agent User Interface are configured by the CDP administrator using the Web Management Interface. Users can manage backup options and restore files and application revisions from the appliance using the Agent User Interface.

The Agent Service runs in the background, handshaking with the appliance, transmitting data to the appliance, and, when using the CDP backup method on a Windows machine, listening for Windows Event Notifications to discover when data has been written to a local disk; triggering the agent to backup the change to the SonicWALL CDP appliance. When changes have been made, the Agent Service transmits 4 KB to 64 KB data blocks (compressed if necessary) to the appliance for backup.

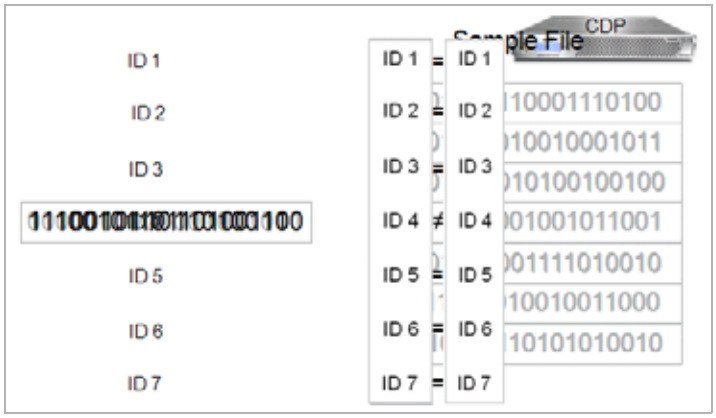
For more information about the SonicWALL CDP Agent User Interface, refer to the "About the Agent User Interface" section on page 94.

About Data De-Duplication

Data de-duplication technology is used on the agent during backups of revisions for both applications and files/folders. This allows all new data to be backed up, while existing data is not rewritten to the appliance. Metadata keeps track of where the changes occur, and is always included with revisions.

Figure 1 shows a graphical representation of the data de-duplication process.

Figure 1 Data De-Duplication



About FileSets

When backing up data, SonicWALL CDP is aware of interdependencies among multiple, related files, called FileSets. Both application backup and backup of files and folders use the concept of FileSets to include all relevant data in backups, so that recovery can provide everything needed for full and seamless operation.

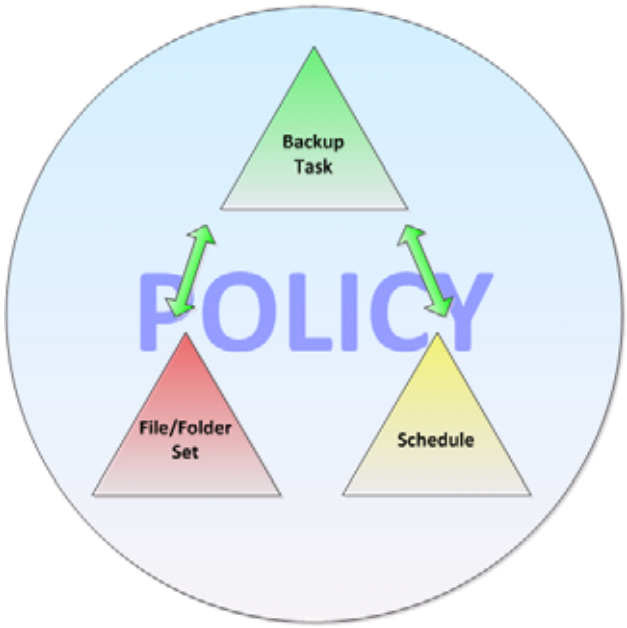
On Windows agents, Microsoft Volume Shadow Copy Service (VSS) is used during backups to take a snapshot of all relevant data, providing a cohesive set of files at a certain point in time. Using the VSS method also eliminates the need to stop services in order to keep files in sync while performing a backup.

How Backup Policies Work

Data backup in SonicWALL CDP is accomplished via policies. Policies control the backup activities performed by SonicWALL CDP.

Figure 2 illustrates a policy for a files and folders backup.

Figure 2 Policy Contents



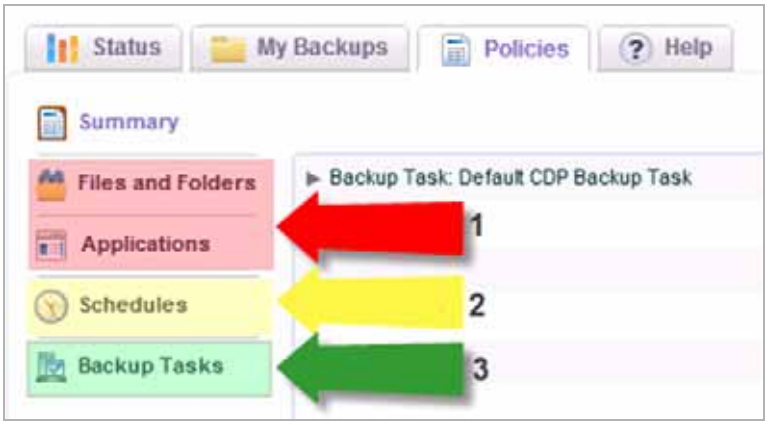
Each backup policy contains one or more backup tasks.

Each backup task consists of two components:

- An Application object or a Files and Folders object that defines what to include in the backup
- A Schedule object that defines when the backups will occur

Figure 3 illustrates the steps for creating a policy.

Figure 3 Creating a Policy



Backup policies are defined both at the administrative level in the Web Management Interface and at the local agent level using the Agent User Interface. Policies can be very granular, even allowing you to create multiple backup tasks in one Files and Folders object, if desired. Such an object can contain more than one folder. You can also define the number of revisions to keep when configuring the backup policy.

About Default Policies for Agents

One or more default policies to be used by agents are defined in the Web Management Interface. A default policy is inherited by each agent connected to the SonicWALL CDP appliance. The CDP administrator can define different default policies for different agents, but each agent will only inherit one default policy from the appliance.

On a newly installed SonicWALL CDP appliance, one Default Policy is predefined. It consists of the legacy style Default CDP Backup Task that contains the Default Folderset Files and Folders backup object and the Default CDP Schedule. The Default CDP Schedule backs up changes whenever they occur on the agent machine. Figure 4 shows the Default Policy, opened for editing.

Figure 4 Default Policy

Edit Policy
Policy Name:
Quota:
80
GB
Quota Type:
Size
Select Continuous Data Protection Task:
Default CDP Backup Task
Select Fileset Tasks and/or Application Tasks:
Administrator's Agent Override:
Optional. Administrator can enable or prevent Agents from backing up undesired Files and Folders. The policy is often used to prevent agents from backing up Movies, Music, Etc.
Default Folderset Files and Folders
OK
Cancel

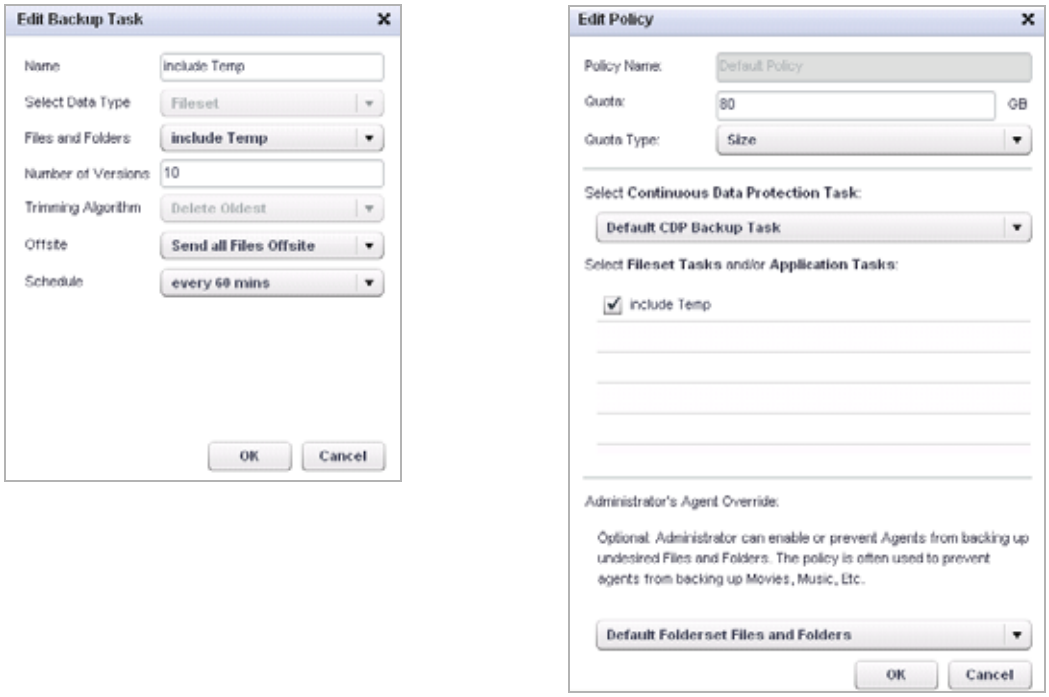
Policy Configuration by the Administrator

A policy can contain more than one backup task. The administrator can edit the predefined default policy or another default policy to add one or more additional backup tasks. This task can be a Fileset or Client Application backup task. The administrator might add such a task to force agents to back up certain files or application data by default, on a certain schedule.

To do this, the administrator first creates the backup task, and then edits the default policy to add it by selecting the checkbox for it. Before creating the backup task, the Files and Folders object must be created, as well as a Schedule object. These objects are included in the backup task.

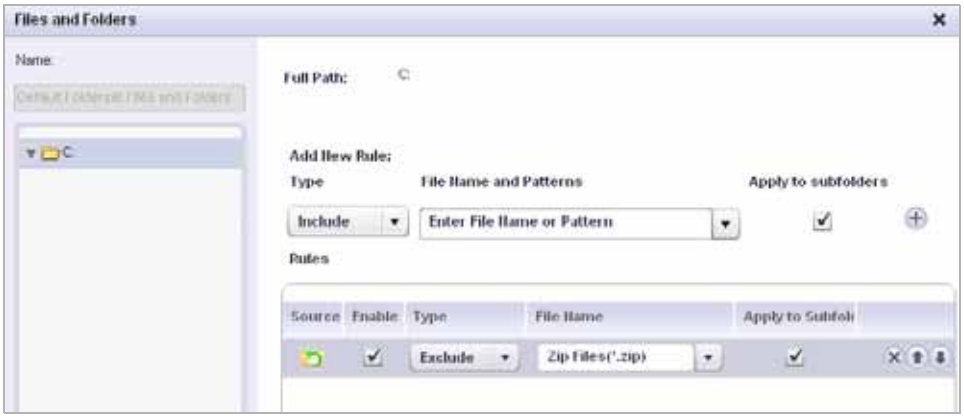
Figure 5 shows an additional backup task and the modified Default Policy that includes it.

Figure 5 Modified Default Policy



The Edit Policy window also provides the Administrator's Agent Override section. The administrator can use this to exclude certain types of files or folders from backup by the agent. The administrator configures the Files and Folders object, such as the Default Folderset Files and Folders object, with a rule to exclude the files or folders. The modified Files and Folders object is then selected for inclusion in the default policy. Figure 6 shows the modified Files and Folders object with a rule to exclude certain file types.

Figure 6 Files and Folders with Excluded File Rule

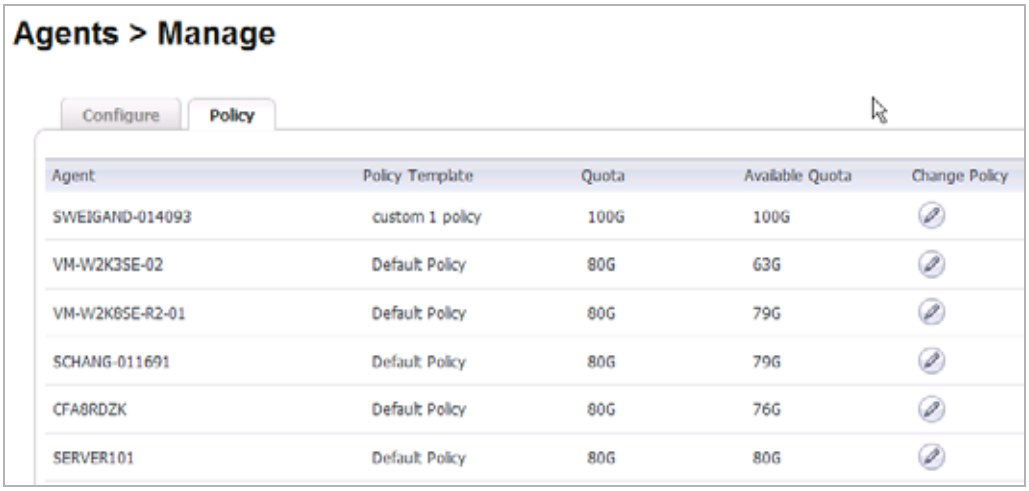


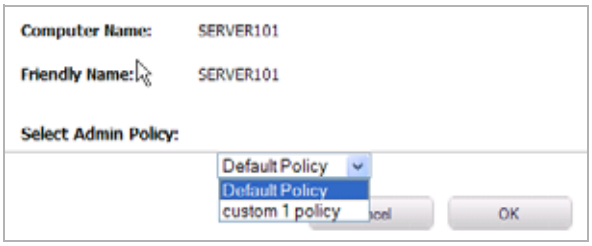
There can be multiple default policies configured on a SonicWALL CDP appliance. The SonicWALL CDP administrator can define different default policies for different agents, but each agent will only inherit one default policy from the appliance.

After creating a new default policy or modifying an existing one, the administrator can apply the policy to certain agents from the Agents > Manage page of the Web Management Interface.

Figure 7 shows the Policy tab of the Agents > Manage page, with the Change Policy configure buttons, and the small popup window that allows the policy selection for that agent.

Figure 7 Changing Default Policy for Agents





In this way, the administrator can define the agent files or applications to back up or exclude, and the schedule for those backups, and can direct the backup policy to be inherited by certain agents.

Policy Configuration by the User

At the agent level, you can edit this default policy to add files and folders for backup. While you can edit the default policy, you cannot delete it. The purpose of the default policy is to allow the administrator to force the backup of certain files and applications on the agent. Deleting the policy would counteract this intent.

A user cannot create a new CDP type backup task via the Agent User Interface. The Agent UI only allows the creation of Fileset or Application backup tasks. Only the administrator can create CDP type backup tasks by using the Web Management Interface.

CDP type backup tasks or policies use Interval scheduling, which back up changed data continuously, or continuously during a set interval, such as from 8am to 5pm Monday through Friday. Fileset or Application backup tasks use Event scheduling only. In contrast to the continuous nature of Interval scheduling, Event scheduling allows you to set recurring times, dates, or days for backups to occur.

A CDP backup task also differs from a Fileset or Application backup task in that the defined files and folders are backed up as separate entities, not as filesets. Trimming of old revisions can also use a different method than is available for Fileset or Application backup policies.

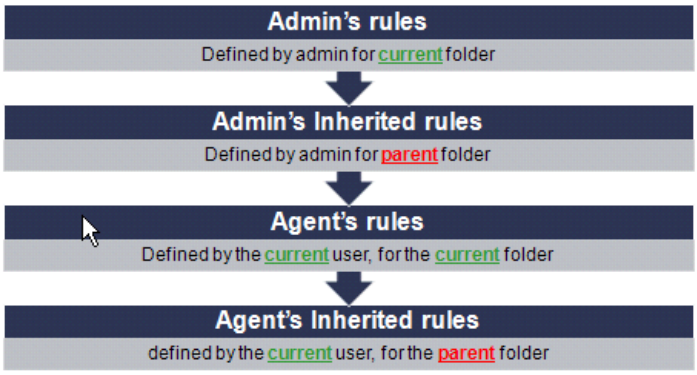
The default CDP type policy is also used for policies transitioned from previous versions of SonicWALL CDP after upgrading.

How Rules Work

The rules within Files and Folders objects are flexible, providing the ability to include or exclude files or folders at any level. Rules are defined at both the administrative level and the agent level, with administrative rules taking precedence over local rules. CDP type objects also provide similar rule functionality. Application objects do not use rules in the same format, but allow you to select the application components to back up, such as individual user mailboxes or system state files.

Figure 8 illustrates the order in which rules are applied when determining what to back up.

Figure 8 Admin vs Agent Rule Precedence

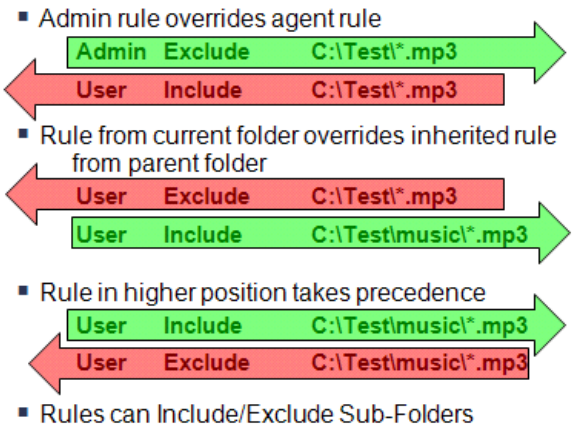

Admin's rules
Defined by admin for current folder
Admin's Inherited rules
Defined by admin for parent folder
Agent's rules
Defined by the current user, for the current folder
Agent's Inherited rules
defined by the current user, for the parent folder

Within the constraints of administrative rule precedence, rules operate as follows:

- Rules from current folder override inherited rules from parent folder
- Rules in higher position take precedence; rule order can be adjusted in the Agent User Interface
- Rules can include or exclude sub-folders

Figure 9 illustrates rule operation and precedence.

Figure 9 Rule Operational Precedence


Admin rule overrides agent rule
Admin Exclude C:\Test*.mp3
User Include C:\Test*.mp3
Rule from current folder overrides inherited rule from parent folder
User Exclude C:\Test*.mp3
User Include C:\Test\music*.mp3
Rule in higher position takes precedence
User Include C:\Test\music*.mp3
User Exclude C:\Test\music*.mp3
Rules can Include/Exclude Sub-Folders

How Scheduling Works

Backups are scheduled using a very flexible interface for schedule configuration. You can schedule backups to occur at any interval down to the minute or up to months apart. Custom, specific dates can be configured.

There are two types of scheduling:

- Event – Uses fixed time points, such as Mondays at 5 PM or midnight every evening. Used for Fileset or Application backup tasks.
- Interval – Uses Always On or always on during a specific start and end time, such as Sundays from 4 PM to 8 PM. Used for CDP type backup tasks.

  Interval scheduling is used for the default CDP type policy on an agent. Because the Agent User Interface does not provide a way to create a new CDP type backup task, you would not have another opportunity to use interval scheduling.

When creating a backup task in the Web Management Interface, the type of Schedule object available for selection depends on whether you have selected **CDP**, **Fileset**, or **Client Application** in the **Select Data Type** field of the Add Backup Task configuration window.

The scheduling interface provides four tabs for different scheduling options:

- Day Interval
- Days of the Week
- Days of the Month
- Specific Dates

Each tab provides configuration fields and a calendar that displays the selected dates with a darker background, so that you can easily verify your configuration.

Figure 10 illustrates the **Day Interval** tab.

Figure 10 Day Interval Scheduling

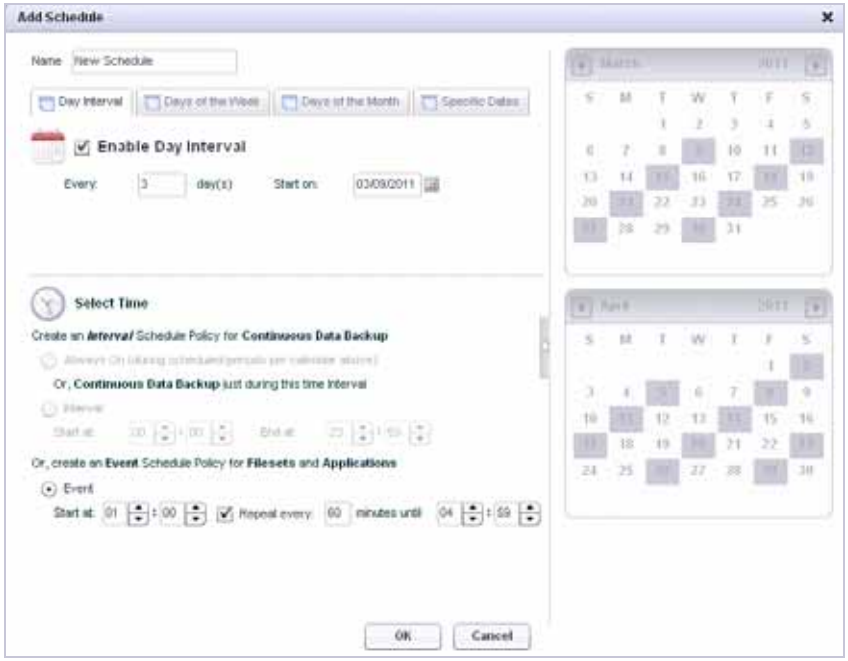

Add Schedule
Name New Schedule
Day Interval
Days of the Week
Days of the Month
Specific Dates
Enable Day Interval
Every: 3 day(s) Start on: 03/09/2011
Select Time
Create an Interval Schedule Policy for Continuous Data Backup
Or, Continuous Data Backup just during this time interval
Or, create an Event Schedule Policy for Filesets and Applications
Event
Start at: 01 : 00 Repeat every: 60 minutes until 04 : 59
OK
Cancel

Figure 11 illustrates the **Days of the Week** tab.

Figure 11 Days of the Week Scheduling

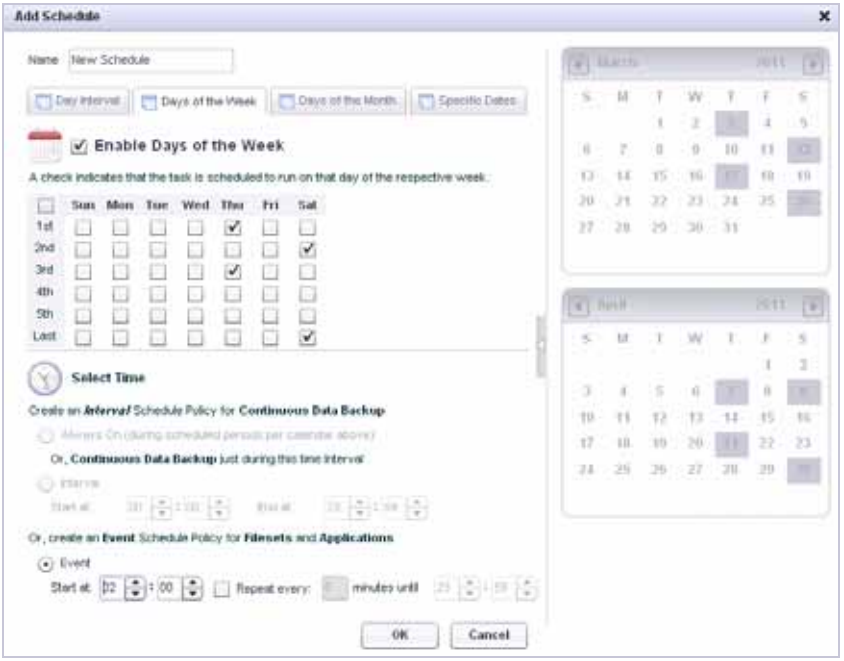


Figure 12 illustrates the **Days of the Month** tab.

Figure 12 Days of the Month Scheduling

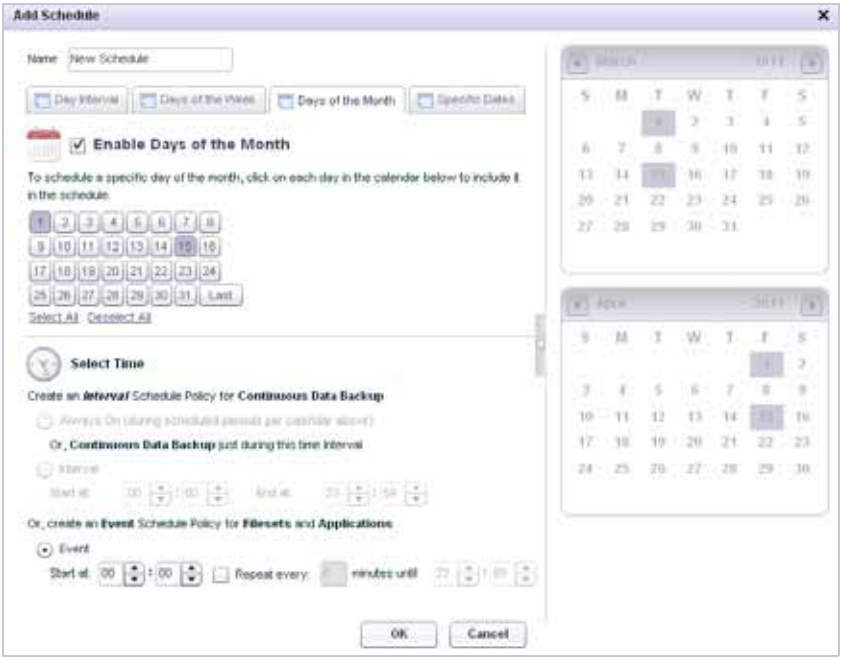
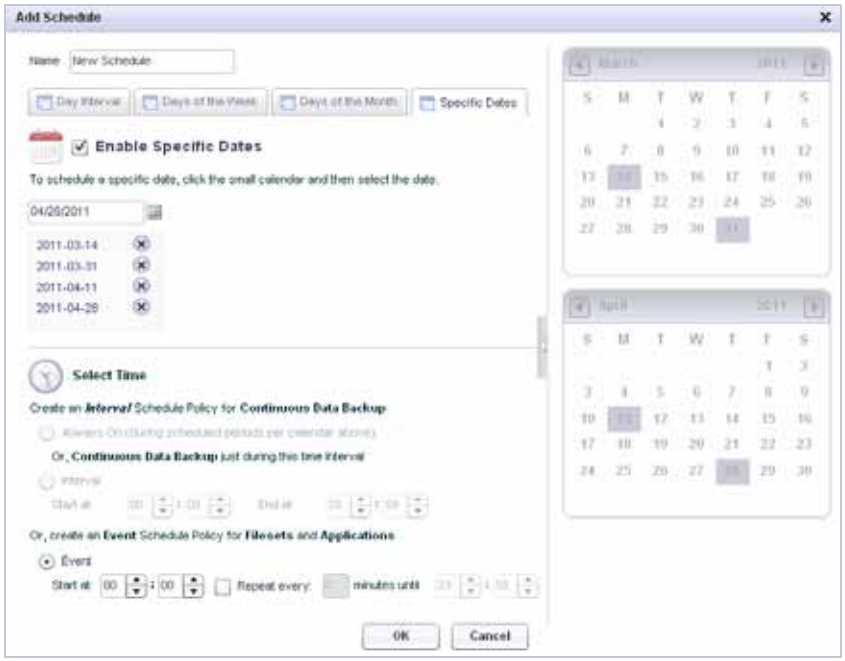

Add Schedule
Name New Schedule
Day Interval
Days of the Week
Days of the Month
Specific Dates
Enable Days of the Month
To schedule a specific day of the month, click on each day in the calendar below to include it in the schedule.
Last
Select All
Deselect All
Select Time
Create an Interval Schedule Policy for Continuous Data Backup
Or, Continuous Data Backup just during this time interval
Or, create an Event Schedule Policy for Filesets and Applications
Event
Start at: 00 : 00
Repeat every:
minutes until
OK
Cancel

Figure 13 illustrates the **Specific Dates** tab.

Figure 13 Specific Dates Scheduling



The same data can be scheduled for backup with multiple policies using different schedules, allowing you to maintain near-continuous revisions along with daily, weekly, monthly, or custom scheduled versions. The number of revisions to keep is controlled by the settings in each policy.

How Bare Metal Recovery Works

Bare Metal Recovery is a separate software tool that creates a disk image backup. A disk image backup includes a backup of operating systems, applications and configuration files, software updates, personal settings and other data.

To use Bare Metal Recovery with the SonicWALL CDP appliance, you use the Web Management Interface to create a user account on the appliance with the desired quota. Then you can launch the Bare Metal Recovery application and save the image to the SonicWALL CDP appliance.

Disk imaging includes images of disk partitions and track zero with the Master Boot Record (MBR). Disk partitions include files and folders (independent of their attributes), boot record, FAT (file allocation table) and root. The Master Boot Record is the code used by the BIOS to load the operating system into memory; residing on track zero of the disk.

Bare Metal Recovery disk image creation is automatic, which means files and folders do not have to be earmarked for backup. To ensure that the backup and recovery processes are streamlined, Bare Metal Recovery disk images only store hard disk parts that contain data.

Bare Metal Recovery images can be backed up directly to the SonicWALL CDP appliance with FTP. Bare Metal Recovery disk images can also be created on local hard disks, CD-R/RW, DVD+R/RW, DVD-RW, or removable media such as Firewire (IEEE-1394) and USB (1.0, 1.1, and 2.0) devices. Once created, the image can later be transferred to any other media. Lost data from the disk image can be retrieved at any time. Additionally, the disk image can be accessed as a virtual drive for browsing and extracting files.

For more information on Bare Metal Recovery, refer to the *Bare Metal Recovery and Local Archiving - Workstation User's Guide*.

How the SonicWALL CDP Offsite Service Works

The **SonicWALL CDP Offsite Service** provides a secure server, or Portal, that stores backed up data for protection against local disaster. During registration of your SonicWALL CDP appliance, you are able to select a North American or European data center. You can also use the Web Management Interface to configure another upstream SonicWALL CDP appliance for offsite backup.

Note The SonicWALL CDP Offsite Service is offered as a subscription-based service.

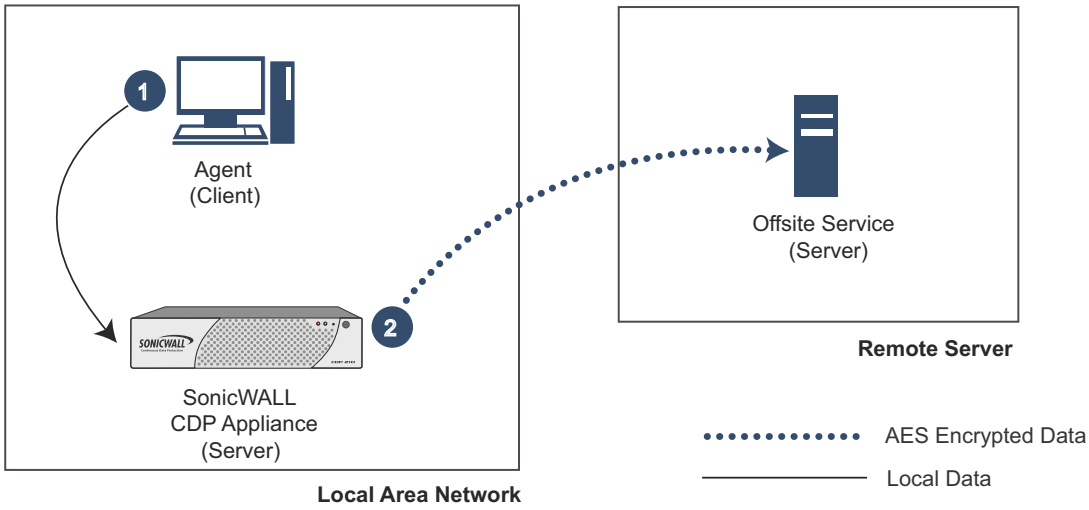
Data transmitted and stored securely at either the North American or European Offsite Service is available for retrieval when onsite data has been destroyed or the onsite appliance has been rendered inoperable, enabling an enterprise to be up and running quickly after a disaster event.

Compressed, full-database and full-file (with latest revision) data blocks are encrypted and transmitted from the SonicWALL CDP appliance to the Offsite Service. Offsite Service communication uses SSL/TLS transport layer encryption, and AES application layer encryption. In the event that a local SonicWALL CDP recovery is not viable, the SonicWALL CDP administrator can recover the data from the Offsite Service using an encryption key.

Data backed up using the SonicWALL CDP Offsite Service is protected by AES (advanced encryption standard) 256-bit encryption, and can only be recovered using an AES 256-bit encryption key, set automatically and available only to the network administrator. Data stored using the Offsite Service is fully secure, as it cannot be decrypted without the key, even by SonicWALL technical support engineers.

Refer to Figure 14 for the Offsite Service data backup flow. For more information about the SonicWALL CDP Offsite Service, refer to the “Site-to-Site Service Overview” section on page 201.

Figure 14 Offsite Service Data Backup Flow

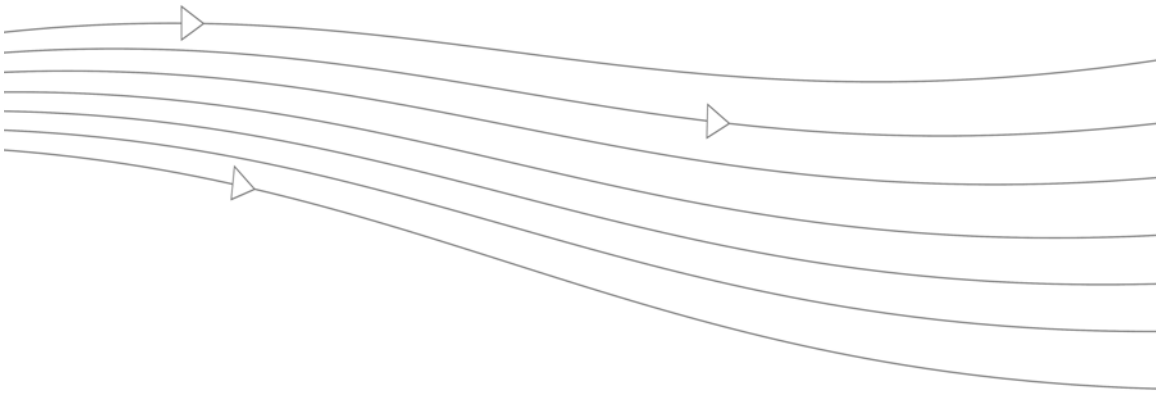


1. The agent sends data blocks (compressed as needed) to the SonicWALL CDP Appliance (local server).
2. The SonicWALL CDP appliance sends AES encrypted data blocks to the Offsite Service (remote server).

How SonicWALL CDP Local Archiving Works

Local archiving is a separate software tool that allows you to archive some or all of the contents of an upstream (offsite) or downstream (local) SonicWALL CDP appliance onto a USB device. This feature can also be used to create a portable backup that can be restored at another site that does not have a SonicWALL CDP appliance. Data can be archived to the USB device in encrypted format.

The Local Archive Manager application is installed on an agent system as part of a Complete installation of the SonicWALL CDP Agent software. For more information about Local Archiving, see the “SonicWALL CDP Local Archiving Overview” on page 215.



Chapter 2: Initializing the CDP Appliance

This chapter provides information about the system requirements and initial configuration process for your SonicWALL CDP appliance. This chapter includes the following sections:

- "Supported Platforms and Deployment Requirements" section on page 21
- "System and Network Requirements" section on page 22
- "Requirements for Supported Applications" section on page 30
- "Registering the SonicWALL CDP Appliance" section on page 31
- "Updating and Managing the SonicWALL CDP Appliance" section on page 35

Supported Platforms and Deployment Requirements

SonicWALL CDP 6.0 is supported on the following platforms:

- SonicWALL CDP 110
- SonicWALL CDP 210
- SonicWALL CDP 220
- SonicWALL CDP 5040
- SonicWALL CDP 5040B
- SonicWALL CDP 6080
- SonicWALL CDP 6080B
- SonicWALL CDP 1440i
- SonicWALL CDP 2440i
- SonicWALL CDP 3440i
- SonicWALL CDP 4440i

System and Network Requirements

This section provides deployment considerations for your agents (client or server) and network requirements. Table 1 lists the minimum system and network requirements.

Table 1 SonicWALL CDP Deployment Requirements

Minimum Client Requirements	• Pentium III Processor • 450 MHZ with at least 256 MB of RAM • 40 MB of free disk space • Microsoft Windows 7, Windows Vista, Windows XP
Minimum Server Requirements	• Intel Celeron 2.0GHZ Process • 256 MB DDR • Microsoft 2008 Server, 2003 Server
Network Requirements	• High speed Internet connection (Serial, DSL, Cable, T1) • Router or hub with wired Ethernet port

About the SonicWALL CDP Appliance

The SonicWALL CDP appliance is a dedicated disk backup appliance that collects data blocks from agents for storage and, if configured, for secure transmission to the Offsite Service storage location. The SonicWALL CDP series has several appliance models that range in capacity, agent support, and additional features. For the SonicWALL CDP 6.0 release, SonicWALL provides the following platforms differentiated by hard disk capacity and the recommended amount of agents:

Generation 4 platforms:

- SonicWALL CDP 210*
- SonicWALL CDP 220
- SonicWALL CDP 5040B
- SonicWALL CDP 6080B

Generation 3 platforms:

- SonicWALL CDP 110
- SonicWALL CDP 210*
- SonicWALL CDP 5040
- SonicWALL CDP 6080

*The SonicWALL CDP 210 is both a Gen 3 and Gen 4 model. The Gen 4 platform has a larger disk capacity.

Generation 2 platforms:

- SonicWALL CDP 1440i
- SonicWALL CDP 2440i
- SonicWALL CDP 3440i
- SonicWALL CDP 4440i

Table 2 provides descriptions of the hardware features common to all Gen 3 and Gen 4 platforms.

Table 2 SonicWALL CDP Hardware Features

Feature	Description
HDD LED (Hard Disk Drive)	Indicates data transfer to and from the hard disk.
Power LED	Indicates the SonicWALL CDP appliance is powered on.
Reset Button	Allows reboot of the SonicWALL CDP appliance.
Power Button	Allows the SonicWALL CDP appliance to power on (one press) or power off (10-second press).
Cooling Fan	Provides optimal air circulation.
AC Power	Allows the SonicWALL CDP appliance to connect to AC power using the supplied power cable.
LAN Port	Allows the SonicWALL CDP appliance to connect to your local area network.
USB Port	Allows a USB device to be plugged in and used for local archiving.

Table 3 provides a comparison of features for the Gen 4 SonicWALL CDP platforms.

Table 3 SonicWALL CDP Gen 4 Platform Comparison

Feature	210	220	5040B	6080B
Recommended number of user agents	25	50	100	250
Recommended number of server agents	5	5	10	15
Hard disk capacity (usable)	860 GB	1.7 TB	5 TB	5 TB Extensible to 10 TB
Internal hard drives	1	1	4	4 Extensible to 8
Chassis model	Mini	Mini	1U	2U
RAID support	Not supported	Not supported	RAID 5	RAID 5
Hot-swappable and Redundant power	Not supported	Not supported	Not supported	Yes
Field Replaceable Hard Drive	Not supported	Not supported	Yes	Yes
Ethernet interface	100 BaseT	100 BaseT	1 GbE	1 GbE
Site-to-Site Backup	Optional	Optional	Optional	Optional
Local Archiving	Included	Included	Included	Included

Table 4 provides a comparison of features for the Gen 3 SonicWALL CDP platforms.

Table 4 SonicWALL CDP Gen 3 Platform Comparison

Feature	110	210	5040	6080
Recommended number of user agents	15	25	60	100
Recommended number of server agents	5	5	10	15
Hard disk capacity (usable)	400 GB	869 GB	2.25 TB	2.25 TB Extensible to 4.5 TB
Internal hard drives	1	1	4	4 Extensible to 8
Chassis model	Mini	Mini	1U	2U
RAID support	Not supported	Not supported	RAID 5	RAID 5
Hot-swappable and Redundant power	Not supported	Not supported	Not supported	Yes
Field Replaceable Hard Drive	Not supported	Not supported	Yes	Yes
Ethernet interface	100 BaseT	100 BaseT	1 GbE	1 GbE
Site-to-Site Backup	Optional	Optional	Optional	Optional
Local Archiving	Included	Included	Included	Included
Bare Metal Recovery Server Licenses	Optional	Optional	1	2
Bare Metal Recovery Workstation Licenses	1	2	5	10

Table 5 provides a summary of features by platform for Gen 2 platforms for comparison.

Table 5 SonicWALL CDP Gen 2 Platform Comparison

Feature	1440i	2440i	3440i	4440i
Recommended number of supported agents	15	30	75	Unlimited
Hard disk capacity	160GB	250 GB	400GB	650GB
Ethernet	1x10/100 Base-T Ethernet	1x10/100 Base-T Ethernet	10/100/1000 GIG LAN	10/100/1000 GIG LAN
Chassis model	Mini	Mini	1U	2U
RAID support	Not supported	Not supported	RAID 1	RAID 5
Encryption	AES 256-bit	AES 256-bit	AES 256-bit	AES 256-bit
Continuous Data Protection	Included	Included	Included	Included
File Versioning	Included	Included	Included	Included
Central Administration	Included	Included	Included	Included
Desktop, Laptop and Server Backup	Included	Included	Included	Included
Remote Administration	Included	Included	Included	Included
Open Files Backup	Included	Included	Included	Included
Policy Based Backup	Included	Included	Included	Included
Active Directory Backup	Not included	Included	Included	Included
SQL Server Support	Not included	Included	Included	Included
MS Exchange Support	Not included	Included	Included	Included

SonicWALL CDP 1440i

The SonicWALL CDP 1440i is a disk-based backup and recovery appliance that offers real-time end-to-end data protection for small businesses. It includes unique features such as instant data recovery and central administration. The CDP 1440i supports servers, PCs and laptops of small business networks up to 15 agents. The appliance has 160 GB capacity and uses AES 256-bit encryption on offsite data security.

Figure 15 provides a front and back bezel photograph of the SonicWALL CDP 1440i appliance.

Figure 15 SonicWALL CDP 1440i

* Pressing the reset button for several seconds will result in a reboot of the SonicWALL CDP appliance.

**Do not plug devices into any ports (other than those indicated) unless explicitly instructed to do so by a SonicWALL technical support representative. Doing so may void your warranty.

The SonicWALL CDP appliance front and back bezel components are described in the following table:

Feature	Description
HDD LED (Hard Disk Drive)	Indicates data transfer to and from the hard disk.
Power LED	Indicates the SonicWALL CDP appliance is powered on.
Reset Button	Allows reboot of the SonicWALL CDP appliance.
Power Button	Allows the SonicWALL CDP appliance to power on (one press) or power off (10-second press).
Cooling Fan	Provides optimal air circulation.
AC Power	Allows the SonicWALL CDP appliance to connect to AC power using the supplied power cable.
LAN Port	Allows the SonicWALL CDP appliance to connect to your local area network.

SonicWALL CDP 2440i

The SonicWALL CDP 2440i is ideal for small businesses and remote offices. Featuring a 250 GB compressed capacity along with standard throughput and AES 256-bit encryption for offsite data security, it provides continuous real-time data protection for servers, laptops and PCs. Differentiating this solution from many of its competitors is its seamless support of most small business database and applications such as SQL Server and Microsoft Exchange without the need to integrate additional software packages.

Figure 16 provides a front and back bezel photograph of the SonicWALL CDP 2440i appliance.

Figure 16 SonicWALL CDP 2440i

* Pressing the reset button for several seconds will result in a reboot of the SonicWALL CDP appliance.

**Do not plug devices into any ports (other than those indicated) unless explicitly instructed to do so by a SonicWALL technical support representative. Doing so may void your warranty

The SonicWALL CDP appliance front and back bezel components are described in the following table:

Feature	Description
HDD LED (Hard Disk Drive)	Indicates data transfer to and from the hard disk.
Power LED	Indicates the SonicWALL CDP appliance is powered on.
Reset Button	Allows reboot of the SonicWALL CDP appliance.
Power Button	Allows the SonicWALL CDP appliance to power on (one press) or power off (10-second press).
Cooling Fan	Provides optimal air circulation.
AC Power	Allows the SonicWALL CDP appliance to connect to AC power using the supplied power cable.
LAN Port	Allows the SonicWALL CDP appliance to connect to your local area network.

SonicWALL CDP 3440i

The SonicWALL CDP 3440i offers enterprise level data backup protection for small-to-medium businesses and remote offices. The high-performance 1U rack-mountable solution is optimized for up to 75 users and unlimited servers. Offering 400GB compressed capacity with RAID 1 along with accelerated throughput and AES 256-bit encryption for offsite data security, it provides continuous real-time data protection for servers, laptops and PCs using policy-based backup, central administration and open file backup. It supports most small business databases and applications such as Microsoft Exchange, SQL Server, Quickbooks, the accounting applications PeachTree and Great Plains, and more.

Figure 17 provides a front and back bezel photograph of the SonicWALL CDP 3440i appliance.

Figure 17 SonicWALL CDP 3440i

* Pressing the reset button for several seconds will result in a reboot of the SonicWALL CDP appliance.

**Do not plug devices into any ports (other than those indicated) unless explicitly instructed to do so by a SonicWALL technical support representative. Doing so may void your warranty.

The SonicWALL CDP appliance front and back bezel components are described in the following table:

Feature	Description
HDD LED (Hard Disk Drive)	Indicates data transfer to and from the hard disk.
Power LED	Indicates the SonicWALL CDP appliance is powered on.
Reset Button	Allows reboot of the SonicWALL CDP appliance.
Power Button	Allows the SonicWALL CDP appliance to power on (one press) or power off (10-second press).
Cooling Fan	Provides optimal air circulation.
AC Power	Allows the SonicWALL CDP appliance to connect to AC power using the supplied power cable.
LAN Port	Allows the SonicWALL CDP appliance to connect to your local area network.

SonicWALL CDP 4440i

The SonicWALL CDP 4440i is a robust 2U rack-mountable backup and recovery solution for branch offices and mid-size organizations. Offering a 650 GB compressed capacity with RAID 5 along with accelerated throughput and AES 256-bit encryption for offsite data security, it provides continuous real-time data protection for unlimited servers, laptops PCs, databases and business applications. IT administrators benefit from central management and file-level visibility into every agent machine connected to the SonicWALL CDP appliance, enabling enforcement of consistent backup policies and control features available to individual end users.

Figure 18 provides a front and back bezel photograph of the SonicWALL CDP 4440i appliance.

Figure 18 SonicWALL CDP 4440i i.

* Pressing the reset button for several seconds will result in a reboot of the SonicWALL CDP appliance.

**Do not plug devices into any ports (other than those indicated) unless explicitly instructed to do so by a SonicWALL technical support representative. Doing so may void your warranty

The SonicWALL CDP appliance front and back bezel components are described in the following table:

Feature	Description
HDD LED (Hard Disk Drive)	Indicates data transfer to and from the hard disk.
Power LED	Indicates the SonicWALL CDP appliance is powered on.
Reset Button	Allows reboot of the SonicWALL CDP appliance.
Power Button	Allows the SonicWALL CDP appliance to power on (one press) or power off (10-second press).
Cooling Fan	Allows optimal air circulation.
AC Power	Allows the SonicWALL CDP appliance to connect to AC power using the supplied power cable.
LAN Port	Allows the SonicWALL CDP appliance to connect to your local area network.

Requirements for Supported Applications

The following applications are supported for backup and restore by the SonicWALL CDP appliance:

- Microsoft Exchange
- Microsoft Active Directory and System State
- Microsoft SQL Server
- Microsoft SharePoint

Microsoft Exchange

The following versions of Microsoft Exchange are supported by SonicWALL CDP:

- Exchange 2010 32-bit, 64-bit (Service Pack 1)
- Exchange 2007 32-bit, 64-bit (Service Pack 1)
- Exchange 2003 32-bit, 64-bit

Refer to the "Backing up Exchange 2010" section on page 126 and the "Backing up Exchange 2007/2003" section on page 139 for more information.

Microsoft Active Directory and System State

Microsoft Active Directory is supported on the following Windows systems:

- Windows Server 2008 32-bit / 64-bit
- Windows Server 2003 32-bit / 64-bit
- Windows 7 32-bit, 64-bit
- Windows Vista 32-bit, 64-bit
- Windows XP 32-bit, 64-bit

Refer to the "Backing up System State and Active Directory" section on page 156 for more information.

See also http://technet.microsoft.com/en-us/library/cc785306%28WS.10%29.aspx.

Microsoft SQL Server

The following versions of Microsoft SQL Server are supported:

- SQL Server 2008 32-bit / 64-bit
- SQL Server 2005 32-bit / 64-bit

Refer to the "Backing up Microsoft SQL Server" section on page 161 for more information.

Microsoft SharePoint

The following versions of Microsoft SharePoint are supported by SonicWALL CDP:

- SharePoint 2010 (Server/Foundation) 64-bit
- SharePoint 2007 (Service Pack 2) 32-bit

Refer to the "Backing Up SharePoint" section on page 151 for more information.

Registering the SonicWALL CDP Appliance

Before using the SonicWALL CDP appliance, you must register and activate it. This section contains the following subsections:

- "Registering the Appliance on MySonicWALL" section on page 31
- "Activating the SonicWALL CDP Appliance" section on page 33

Registering the Appliance on MySonicWALL

The SonicWALL CDP appliance must be registered on MySonicWALL with the firmware license key before first use. In order to register using the Registration Code obtained from MySonicWALL, you need to configure the appliance's network settings to be able to access the Internet.

If the appliance is not Internet accessible, then you can register the serial number on MySonicWALL, copy the Manual Keyset provided there, and enter the Manual Keyset on the appliance to register instead of applying the Registration Code.

Perform the following steps to register your SonicWALL CDP appliance:

Step 1 Turn on your SonicWALL CDP appliance.

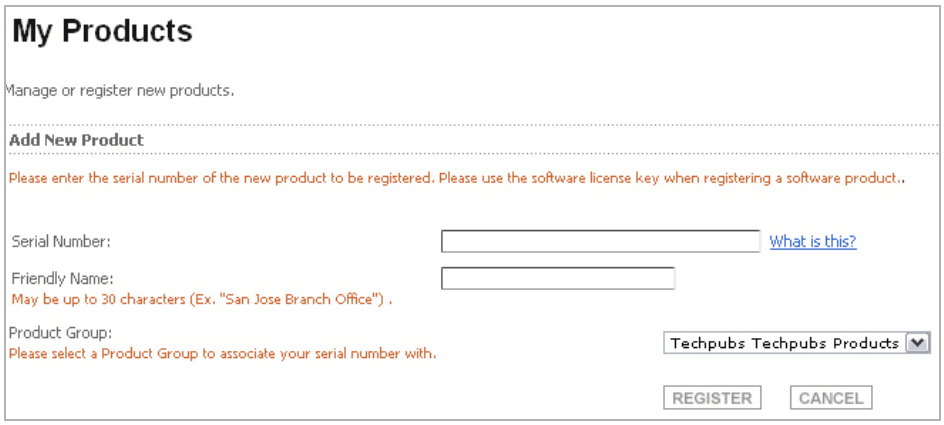
Step 2 Open a Web browser on the computer you are using to manage the SonicWALL CDP and go to <http://www.mysonicwall.com>.

Step 3 Enter your MySonicWALL account **Username** and **Password** in the appropriate fields and click the **Submit** button.

Note You need a MySonicWALL account to register the SonicWALL CDP appliance.

Step 4 Navigate to **My Products** in the left-hand navigation bar.

Step 5 Complete the fields on the My Products page as described in the table below:


My Products
Manage or register new products.
Add New Product
Please enter the serial number of the new product to be registered. Please use the software license key when registering a software product..
Serial Number:
What is this?
Friendly Name:
May be up to 30 characters (Ex. "San Jose Branch Office") .
Product Group:
Please select a Product Group to associate your serial number with.
Techpubs Techpubs Products
REGISTER
CANCEL

Field	Description
Serial Number	Enter the serial number, found on the back or bottom of your SonicWALL CDP appliance.
Friendly Name	Enter a friendly name for your SonicWALL CDP appliance.
Product Group	Select a product group from the drop-down menu. This product group is a logical collection of SonicWALL products that are managed by a user group, defined on MySonicWALL.
Authentication Code	Enter your authentication code, found on the back or bottom of your SonicWALL CDP appliance (just below the serial number).

Step 6 A dialog requesting an offsite backup location appears. Select an offsite backup location from the **Location** drop-down menu.

If you change the offsite data backup location, the data that was saved in the previous location is lost.

Step 7 Click the **Register** button. A confirmation appears with a **Registration Code**. Make a note of the registration code.

For an appliance without Internet access, display the **Manual Keyset**. You can copy the keyset to your clipboard and then to a file, for use when activating your SonicWALL CDP appliance.

Note The registration code or manual keyset are required for activating your SonicWALL CDP appliance in the Web Management Interface.

Activating the SonicWALL CDP Appliance

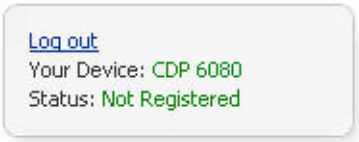
Perform the following steps to activate your SonicWALL CDP appliance. An Internet connection is needed to use the product registration code. If no Internet connection is available, you can use the manual keyset. Both the registration code and manual keyset are acquired in the "Registering the Appliance on MySonicWALL" section on page 31.

To activate your SonicWALL CDP appliance, perform the following steps:

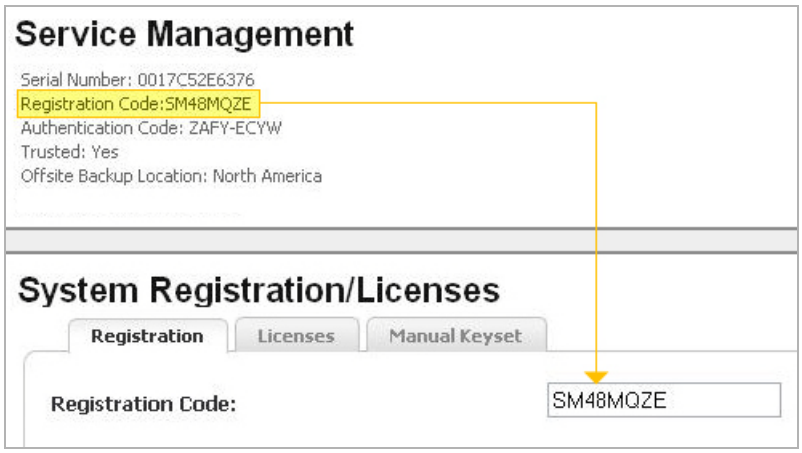
Step 1 Log into the SonicWALL CDP Web Management Interface.

Step 2 Enter "admin" in the **Username** field and "password" in the **Password** field, then click **Login**. These credentials are the default credentials for the appliance. They can be configured later to the desired username and password.

Step 3 The status panel will display the appliance's registration status as Not Registered.

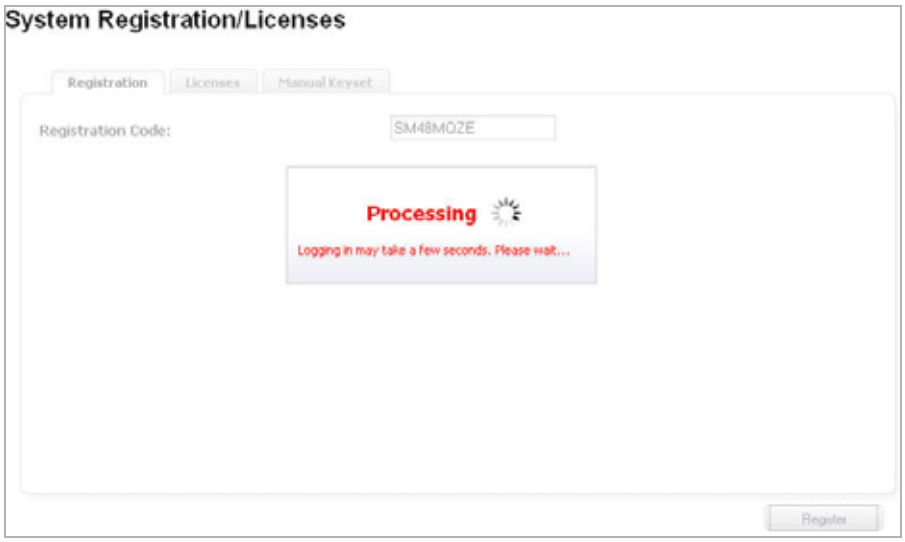


Step 4 Navigate to **System > Registration/License**. On the Registration tab, enter the **Registration Code** in the Registration Code field.



Step 5 If using the manual keyset instead of the registration code, enter it on the **Manual Keyset** tab.

Step 6 Click the **Register** button after entering the registration code. A processing indicator appears.



Your SonicWALL CDP appliance is now registered and fully operational. The status panel and the Registration/Licenses page now displays the current registration status of your SonicWALL CDP appliance.

Step 7 As a best practice, navigate to the **Network > Settings** page and manually update the friendly name of the appliance to match the registered friendly name.

Updating and Managing the SonicWALL CDP Appliance

Updating your SonicWALL CDP Appliance ensures optimum, continuous protection. This section contains the following subsections:

- "Checking Firmware and Software Updates" section on page 35
- "Storing the Offsite Service Encryption Key" section on page 35
- "Resetting a Lost Password" section on page 35

Checking Firmware and Software Updates

The SonicWALL CDP automatically searches for and installs firmware and software updates at startup, and again every six hours. If SonicWALL releases a new firmware version or update, it will be automatically located and installed.

Storing the Offsite Service Encryption Key

The AES 256-bit encryption key protects data being securely transmitted to the Offsite Service. The administrator may view the encryption key using the Web Management Interface.

To view and store your encryption key, perform the following steps:

Step 1 Log into the Web Management Interface and navigate to **System > Settings**.

Step 2 Select the **Offsite** tab.

Step 3 Copy the encryption key located in the Encryption Key field to your computer clipboard. You can then paste the key to a file, or print a copy of the key, for storage.

Note Print the encryption key and store it in a secure location, such as a bank or vault. Data stored at the Offsite Service cannot be recovered without the encryption key, even by SonicWALL technical support engineers.

The encryption key cannot be reset.

If you switch your Offsite destination between the SonicWALL Offsite Portal and another upstream SonicWALL CDP appliance, the displayed encryption key will change accordingly.

See the "Site-to-Site Service Overview" section on page 201 for more information about the Offsite service.

Resetting a Lost Password

If you lose or forget the admin account password for the SonicWALL CDP appliance, you can reset it from the Login screen, but cannot set a new password there. Instead, you must contact SonicWALL Technical Support to get a new one.

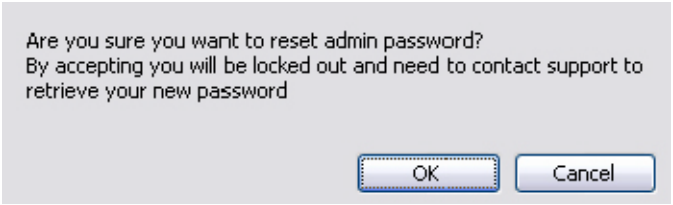
Alternatively, you can reboot the appliance, press any key when prompted by GRUB, and select the SonicWall Authentication Reset option. For details on this method, see "Example Use Case: Authentication Reset" on page 240.

To reset a lost password from the Login screen, perform the following steps:

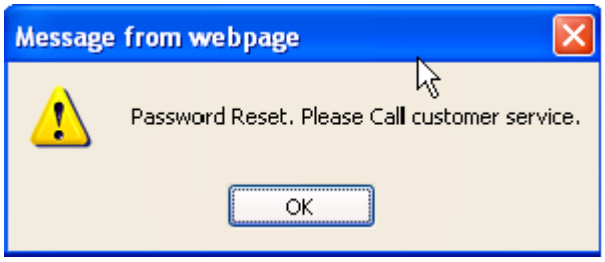
Step 1 Launch the SonicWALL CDP Web Management Interface.

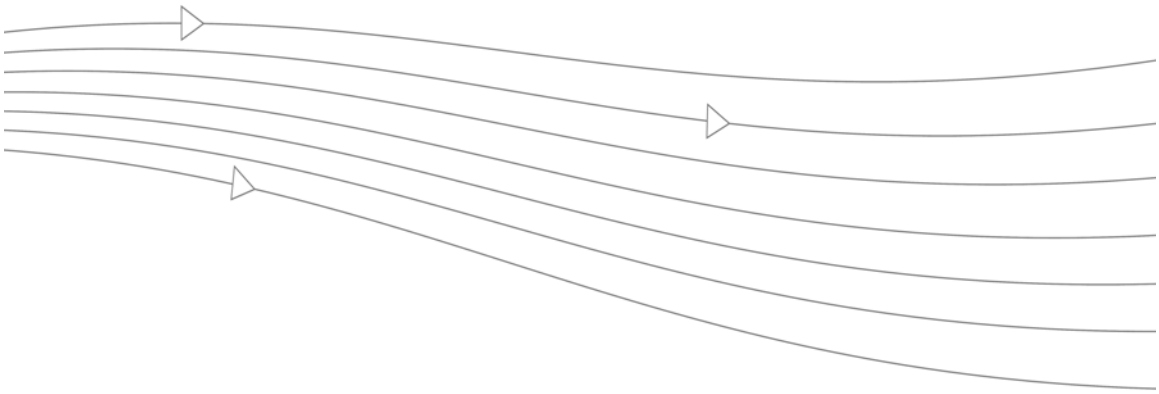
Step 2 Click the **LOST PASSWORD?** link on the Login screen.

Step 3 You will be prompted to confirm the reset action. Click **OK** to confirm or **Cancel** to cancel.


Are you sure you want to reset admin password?
By accepting you will be locked out and need to contact support to retrieve your new password
OK
Cancel

Step 4 A confirmation dialog informs that the password has been reset, and to contact Support for a new password.





Chapter 3: Configuring System Settings

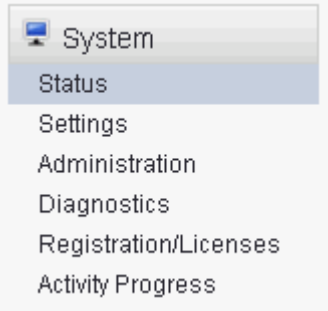
The System pages in the SonicWALL CDP Web Management Interface allow the administrator to view system status and diagnostics, configure system and administrative settings, perform registration, licensing, and upgrades, purge data from the appliance, and restart the appliance. This chapter provides information about the available features on the System pages.

See the following sections:

- “System Interface Overview” section on page 38
- “Understanding the System Status” section on page 39
- “Understanding System RAID” section on page 40
- “Configuring the System Settings” section on page 42
- “Administrative System Tasks and Settings” section on page 55
- “System Diagnostics” section on page 59
- “System Licenses and Registration” section on page 60

System Interface Overview

This section provides a brief overview of the System pages. The System pages in the SonicWALL CDP Web Management Interface allow the administrator to view system status and RAID status, configure system and administrative settings, configure settings for Offsite backup, restore from Offsite, view diagnostic information, perform registration, licensing, and upgrades, purge data from the appliance, and restart the appliance.

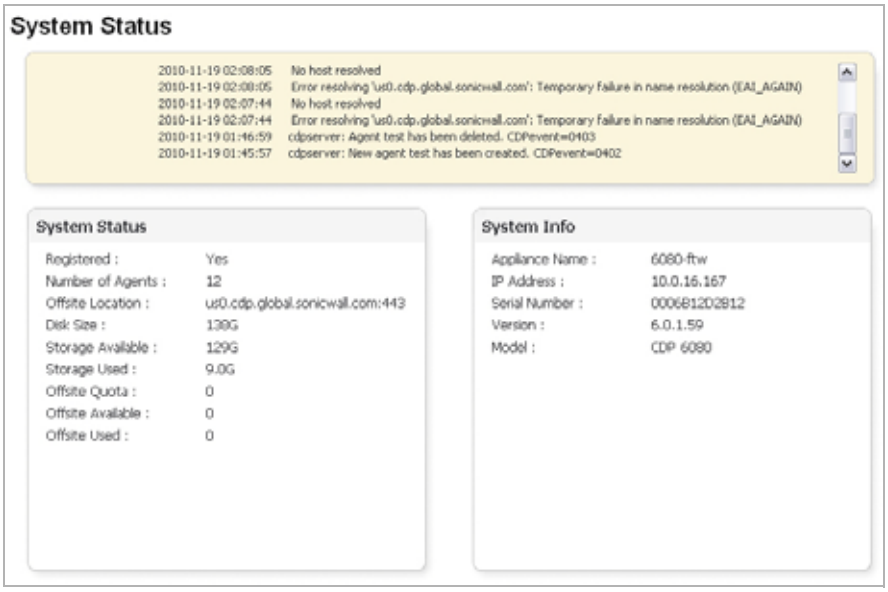


System Control	Description
Status	Provides a display of system messages, alerts, system information and CDP data. System information includes the appliance model number and serial number, CPU description, total memory, up time, version, and operating system type.
RAID (only on selected appliance platforms)	Provides a graphical and textual display of the RAID (Redundant Array of Independent Disks) status for the hard drives on the SonicWALL CDP appliance.
Settings	Allows the administrator to configure passwords, mail settings, alerts, Global Management Services (GMS), and Offsite services. Also allows the administrator to restore from the Offsite service.
Administration	Allows the administrator to check for upgrades, purge data, reset the appliance, and import or export policy and system settings.
Diagnostics	Provides the administrator with a view of CPU information, interfaces, memory utilization, network information, appliance processes, and storage statistics.
Registration/Licenses	Displays license information, registration status, and manual keysets.
Activity/Progress	Allows the administrator to view activity and progress of data transfer to an offsite location.

Understanding the System Status

The **System > Status** page provides a system summary for the SonicWALL CDP appliance and basic usage statistics for all attached agents.

The Status page allows the administrator to view the general status of the appliance and its configured agents. The left pane provides **Administrative Settings**, which provides basic information about the appliance, disk usage, offsite settings and default policy. The right side of the Status page has two tabs: **Activity** and **Agent Summary**. The **Activity** tab provides information about CDP processes, including Disk Space Saver, Revision Limiter, and Offsite Uploader. The **Agent Summary** tab provides summaries by agent including disk space used, disk space available, and number of files backed up.


System Status
2010-11-19 02:08:05 No host resolved
2010-11-19 02:08:05 Error resolving 'us0.cdp.global.sonicwall.com': Temporary failure in name resolution (EAI_AGAIN)
2010-11-19 02:07:44 No host resolved
2010-11-19 02:07:44 Error resolving 'us0.cdp.global.sonicwall.com': Temporary failure in name resolution (EAI_AGAIN)
2010-11-19 01:46:59 cdpserver: Agent test has been deleted. CDPevent=0403
2010-11-19 01:45:57 cdpserver: New agent test has been created. CDPevent=0402
System Status
Registered : Yes
Number of Agents : 12
Offsite Location : us0.cdp.global.sonicwall.com:443
Disk Size : 139G
Storage Available : 129G
Storage Used : 9.0G
Offsite Quota : 0
Offsite Available : 0
Offsite Used : 0
System Info
Appliance Name : 6080-ftw
IP Address : 10.0.16.167
Serial Number : 0006B12D2B12
Version : 6.0.1.59
Model : CDP 6080

The following tables provide a description of the fields in the Status window.

System Status Panel

Field	Description
Registered	Displays the current registration status. • If the appliance is registered, “Yes” is displayed. • If the appliance is not registered, “No” is displayed.
Number of Agents	Displays the number of agents currently assigned to the SonicWALL CDP appliance.
Offsite Location	Displays the address to the current offsite location.
Disk Size	Displays the total amount of local disk space available.
Storage Available	Displays the amount of local disk space available, in megabytes.
Storage Used	Displays the amount of local disk space currently being used, in megabytes.
Offsite Quota	Displays the current disk space quota for the SonicWALL CDP appliance.

Field	Description
Offsite Available	Displays the amount of offsite (remote) quota available, in megabytes.
Offsite Used	Displays the amount of offsite (remote) quota currently being used, in megabytes.

System Info Panel

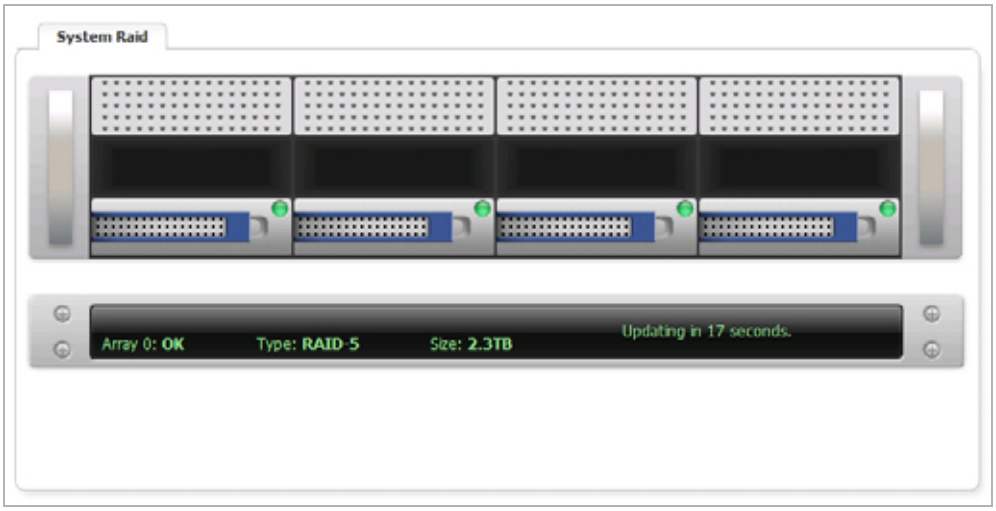
Field	Description
Appliance Name	Displays the name of the current SonicWALL CDP appliance.
IP Address	Displays the IP address of the current SonicWALL CDP appliance.
Serial Number	Displays the serial number of the current SonicWALL CDP appliance.
Version	Displays the current firmware version of the Sonicwall CDP appliance.
Model	Displays the model of the current SonicWALL CDP appliance.

Understanding System RAID

The System RAID page provides a graphical and textual display of the RAID status for the hard drives on the SonicWALL CDP appliance. The page refreshes the status display every 30 seconds.

The System RAID page is available only on appliances that have a RAID controller, including the SonicWALL CDP 6080 and 5040. Some earlier models also provide RAID. The System > RAID page for a SonicWALL CDP 6080 is shown in Figure 1:

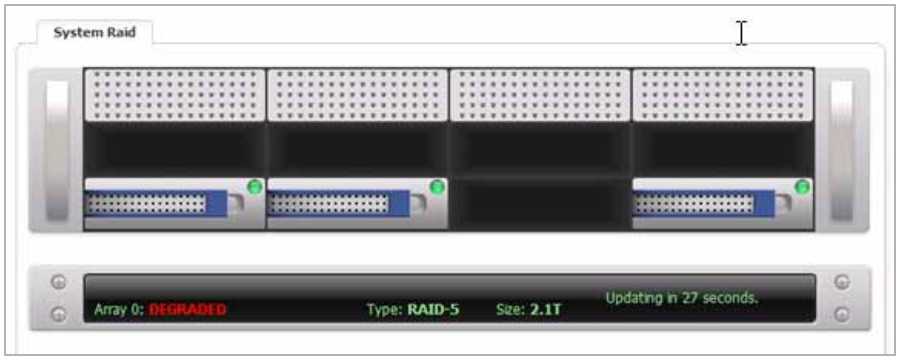
Figure 1 System > RAID Page



The SonicWALL CDP 6080 can operate with either four or eight hard drives, while the SonicWALL CDP 5040 accommodates four drives. In SonicWALL CDP 6080 with four drives, the drives in the secondary array are shown as cover plates at the top of the graphic, as in Figure 1.

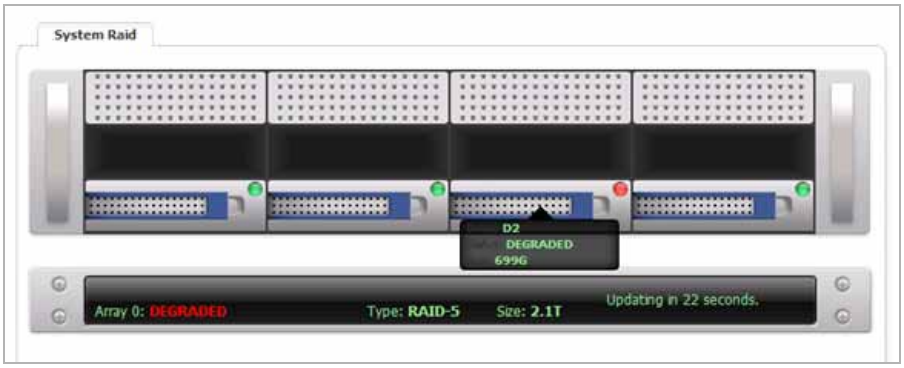
If there is any problem with the RAID configuration on any of the drives, the display will indicate the status of the drive. RAID will continue to function normally when one drive is impaired or removed, but data can be lost if two or more drives are unavailable to the RAID controller. Figure 2 shows a removed drive.

Figure 2 Drive Removed



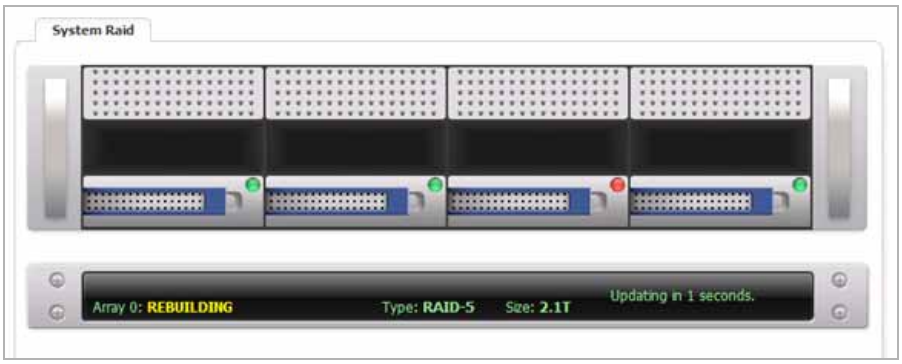
When the drive is replaced, the display indicates the replacement, but the status remains as Degraded until the array begins rebuilding. Figure 3 shows a replaced drive.

Figure 3 Drive Replaced



Soon after replacing the drive, the RAID array begins rebuilding, shown in Figure 4.

Figure 4 Array Rebuilding



For information about the using the RAID related commands available in the SonicWALL CDP command line interface, see the "Command Line Interface Reference" section on page 236.

If a SonicWALL CDP 6080 Expansion Pack is installed, the secondary array along the top of the image will display the status of those drives. For full instructions on installing the Expansion Pack, see the *SonicWALL 6080 Getting Started Guide*.

For information about replacing a single hard drive on the SonicWALL 6080 or 5040 appliance, see the *SonicWALL 6080 Getting Started Guide* or *SonicWALL 5040 Getting Started Guide*.

Configuring the System Settings

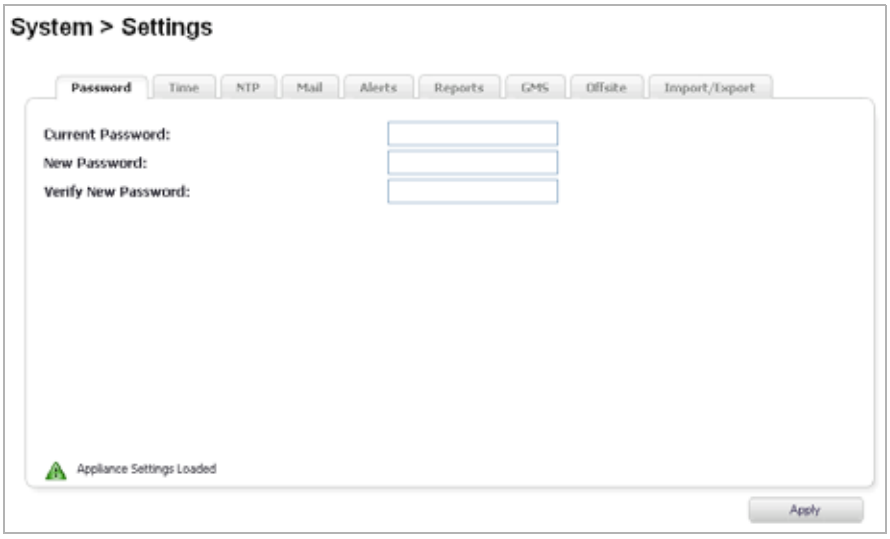
Configuring the System Settings allows the administrator to change passwords, configure time and NTP settings, configure email alerts, configure settings for reports, enable GMS, define Offsite options, and import or export configuration preference settings. This section contains the following subsections:

- "Changing the Password" section on page 42
- "Configuring Time Settings" section on page 43
- "Configuring NTP Settings" section on page 44
- "Configuring Administrative Email Settings" section on page 45
- "Specifying Alerts" section on page 46
- "Configuring Reports Settings" section on page 47
- "Adding a SonicWALL CDP Appliance to GMS" section on page 49
- "Configuring the Offsite Service" section on page 52
- "Exporting or Importing Preferences" section on page 54

Changing the Password

Follow these steps to change your password in the Web Management Interface.

Step 1 Navigate to **System > Settings**. Three fields, **Current Password**, **New Password,** and **Verify New Password**, are visible in the **Password** tab.



Step 2 Type the current password into the **Current Password** field. The default is "password".

Step 3 Specify the desired password in the **New Password** field.

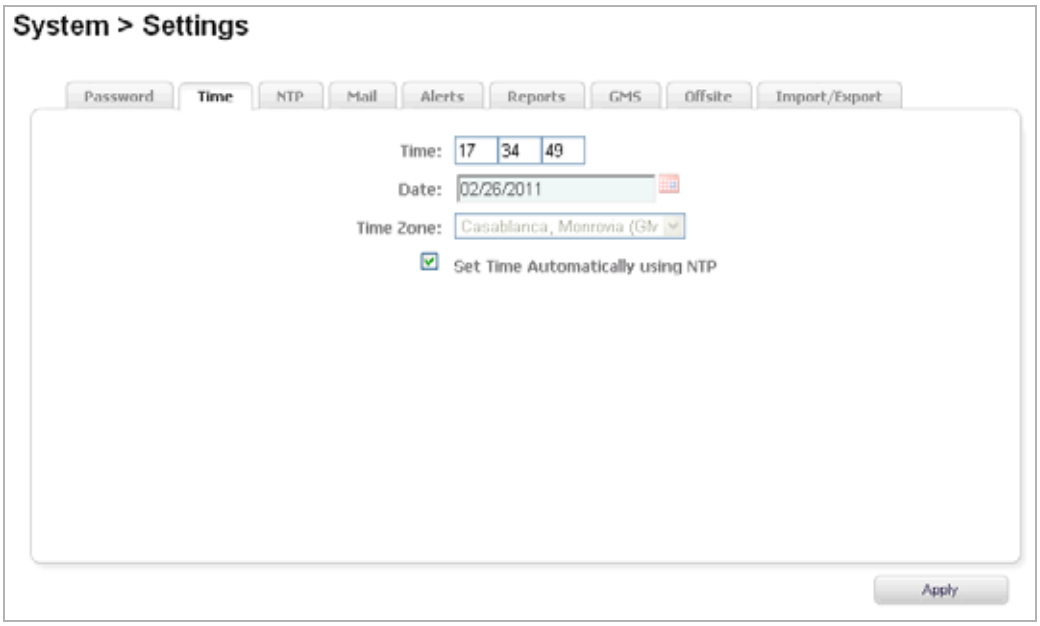
Step 4 Re-enter the desired password in the **Verify New Password** field and click **Apply**. You will automatically log out of the Web Management Interface.

Step 5 Log back in with your username and new password to confirm the password change.

Configuring Time Settings

You can manually set the system time, date, and time zone on the **Time** tab on the System > Settings page or you can configure the system to use Network Time Protocol (NTP) and configure the NTP servers.

Step 1 Navigate to the **System > Settings** page and click the **Time** tab.



Step 2 Specify the desired time, date, and time zone.

Field	Description
Time	Select the time (hh:mm:ss) using the arrow icons. The time will be displayed in 24 hour format.
Date	Specify the date (month, day, year) by entering the desired date in the text field, or use the calendar icon to select a date.
Time Zone	Select your local time zone from the drop-down menu.
Set time automatically using NTP	Check this box to allow the time to be set automatically using NTP.

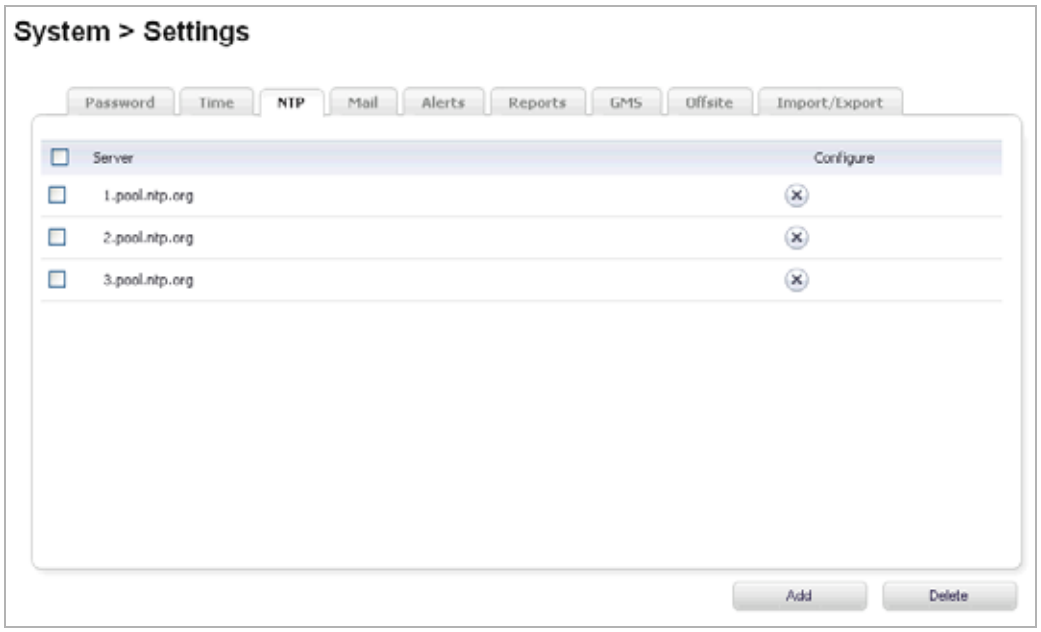
If specific NTP Settings are desired, click on the **NTP** tab to add server addresses.

Step 3 Click the **Apply** button to save the changes. Your SonicWALL CDP appliance is now set to your local time. If the Web Management Interface logs you out, simply log in again.

Configuring NTP Settings

You can configure Network Time Protocol (NTP) servers on the **NTP** tab on the System > Settings page. If NTP is enabled on the **Time** tab, the selected NTP servers will automatically set the system time, date, and time zone for the appliance.

Step 1 Navigate to the **System > Settings** page and click the **NTP** tab.



Step 2 To select one or more of the listed NTP servers to be used by the appliance, select the checkboxes for the desired servers or select the **Server** checkbox to select all NTP servers in the list.

Step 3 To delete an NTP server from the list, click the **X** button for that row. To delete multiple NTP servers, select their checkboxes and then click the **Delete** button at the bottom of the page.

Step 4 To add another NTP server, click the **Add** button.

Step 5 In the NTP dialog box, type the URL for the NTP server into the **server** field and then click **Save**.

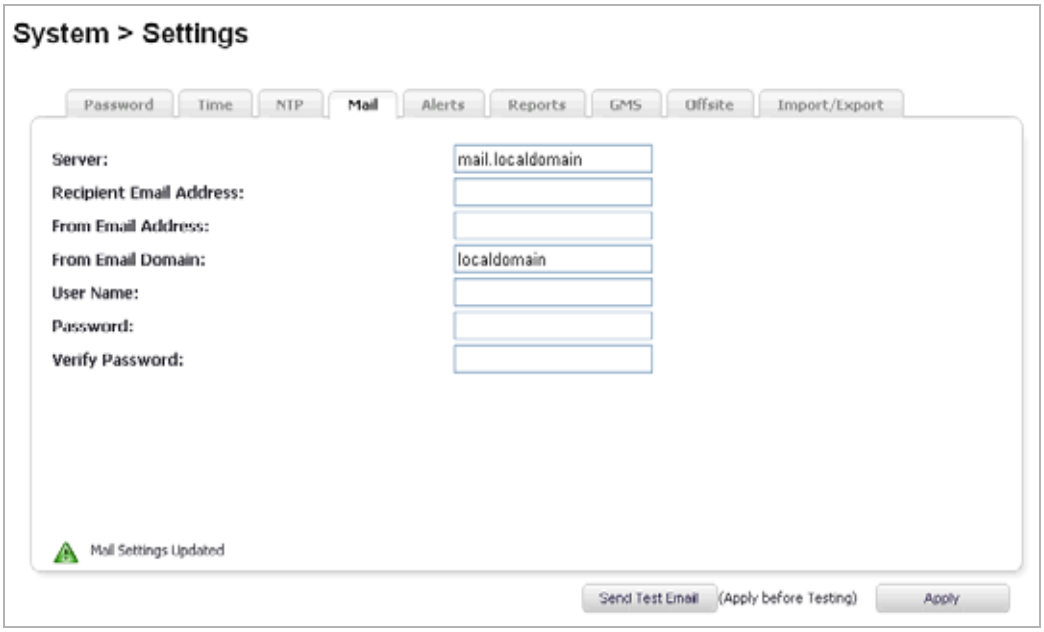
The new NTP server appears in the list.

Configuring Administrative Email Settings

This section provides configuration instructions specific to the System > Mail page in the Web Management Interface. This page allows you to configure email settings so that you can receive alerts.

To configure email settings:

Step 1 Navigate to **System > Settings** in the left-hand menu. Select the **Mail** tab.



Step 2 Provide the following SMTP information:

- **Server (name or IP address)**: Provide the SMTP mail server or IP address. For example, mail.mycompany.com.
- **Recipient Email Address:** Specify the email address where the alert will be sent. For example, administrator_1@mycompany.com.
- **From Email Address**: Specify the email address that will appear as the sender of the email. For example, administrator_2@mycompany.com
- **From Email Domain**: Specify the email domain that will appear in the sender's email address. For example, mycompany.com.
- **User Name (if required)**: Specify a user name associated with the email address you specified in **From email address**, if required. For example, administrator_2.
- **Password (if required)**: Specify a password associated with the email address you specified in **From email address**, if required.

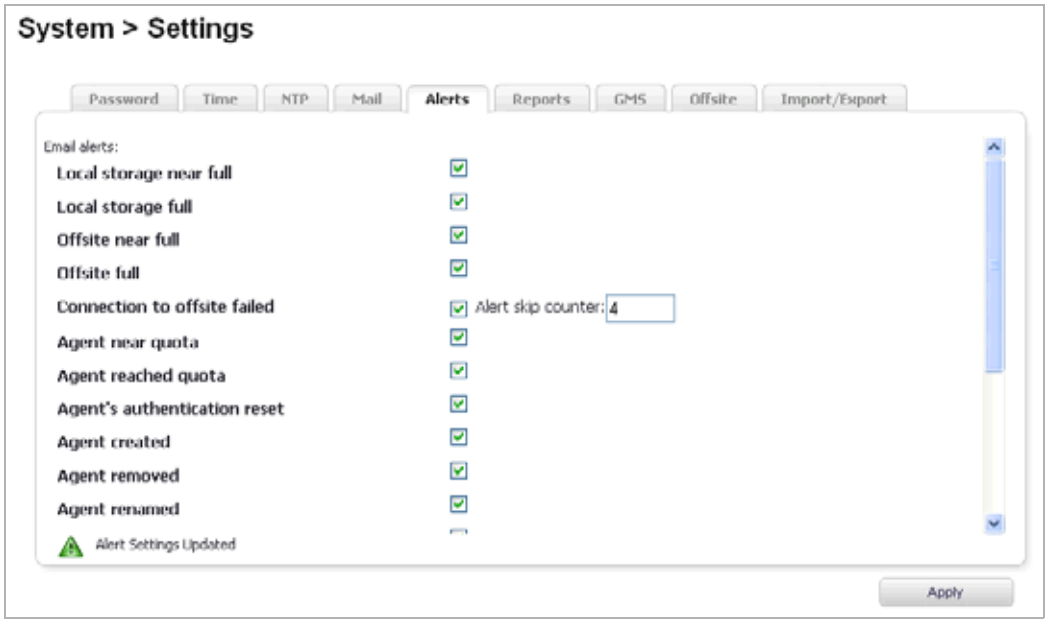
Step 3 Select Apply to save these settings. Click the **Send Test Email** button to send a test email for verification.

Step 4 Check the email account you specified in **Recipient Email Address** to verify that the email was delivered.

Note If you did not receive your test email, verify that you have provided the correct credentials, that you have Internet connectivity, and that the mail server you specified is available. Failed emails will be stored and sent when a mail server connection is established.

Specifying Alerts

The **Alerts** tab in the System > Settings page allows you to specify the type of alerts to receive.



System Settings Alerts Options

Select the checkboxes to receive any of the following alerts:

- **Local storage near full** – The local CDP appliance is nearly full.
- **Local storage full** – The local CDP appliance is completely full.
- **Offsite near full** – The offsite CDP appliance is nearly full.
- **Offsite full** – The offsite CDP appliance is completely full.
- **Connection to offsite failed** – The local CDP appliance cannot connect to the offsite unit.
- **Agent near quota** – The agent has nearly reached its data backup quota on the CDP.
- **Agent reached quota** – The agent has reached its data backup quota on the CDP.
- **Agent's authentication reset** – The agent credentials have changed.
- **Agent created** – A new agent has connected to the CDP.
- **Agent removed** – An agent has disconnected from the CDP.
- **Agent renamed** – An agent has been renamed.
- **Admin password reset** – The CDP admin account password has been changed.
- **Local archive backup failed** – A local archive backup has failed.
- **Local archive backup completed** – A local archive backup has completed successfully.
- **RAID degraded** – A hard drive in the RAID array has a problem or has been removed.
- **Policy invalid** – An invalid policy has been configured or applied.

- **Agent backup failed** – A backup of data from an agent has failed.
- **Agent resource limit** – System resources on an agent are low or exhausted.
- **Re-parse point encountered** – A symbolic link has been backed up, but the object it points to is not backed up.

Alerts are emailed to the configured account. An **Agent backup failed** alert email for a failed file upload to the CDP looks like this:

Subject: Alerts from CDP appliance: RTCDP6.0-DS (Serial# 0006B12D31C1)

Date	Time	Source	Message
2011-02-09	23:10:37	10.128.1.119	CDPAgent:[TELLAKULA-01206] Path, C: (0x00000000), does not exist or is not a directory. (0x00000057)

A **Local archive backup completed** alert looks like this:

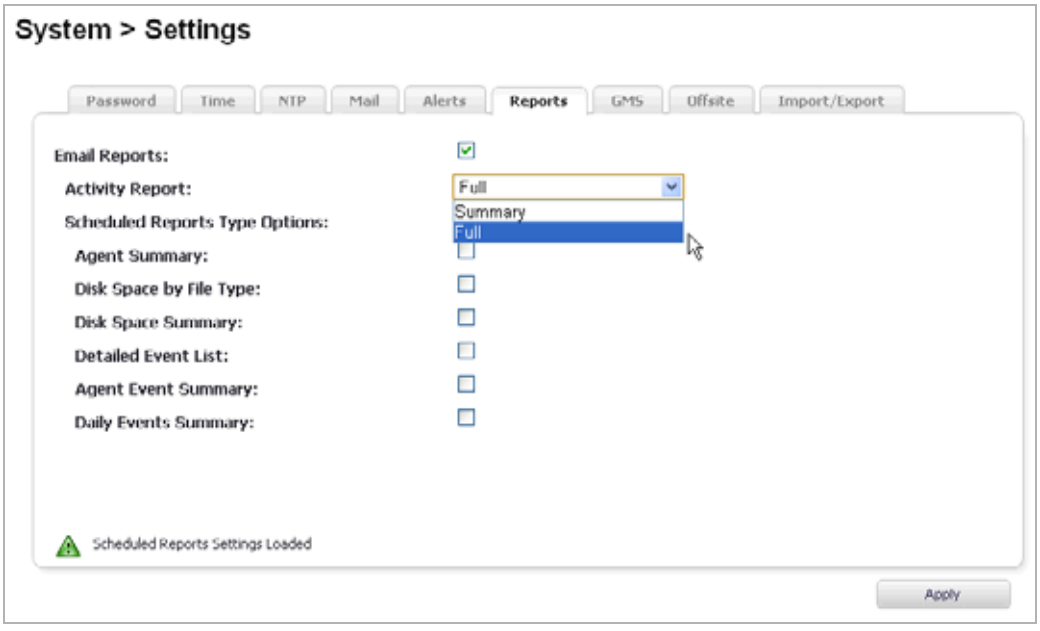
Subject: Alerts from CDP appliance: RTCDP6.0-DS (Serial# 0006B12D31C1)

Date	Time	Source	Message
2011-02-18	10:57:16	rtds	cdpserver: On 2/18/2011 10:57:16 AM, local archiving is completed: 1 agent(s), 3 file(s) were archived successfully, 0 file(s) were skipped. CDPevent=0635
2011-02-18	10:59:52	rtds	cdpserver: On 2/18/2011 10:59:52 AM, local archiving is completed: 1 agent(s), 3 file(s) were archived successfully, 0 file(s) were skipped. CDPevent=0635

Configuring Reports Settings

The **Reports** tab on the System > Settings page allows you to configure the CDP appliance to email Activity reports or scheduled reports of various types.

Step 1 Navigate to the **System > Settings** page and click the **Reports** tab.



Step 2 Select the **Email Reports** checkbox to activate the other options.

Step 3 Select either **Full** or **Summary** in the **Activity Report** drop-down list. Full reports provide more detail than Summary reports.

Step 4 Select the checkbox for each type of report you wish to receive:

- **Agent Summary**

Agent Summary Table

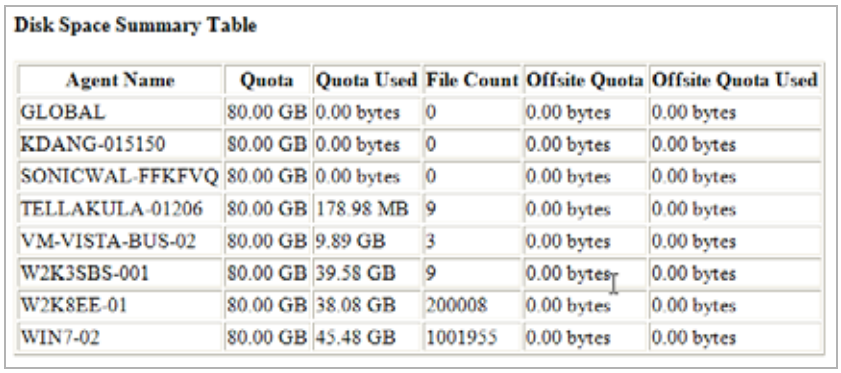
Agent Name	Quota	Total Size	Size On Disk	File Count	Fileset Total	Fileset Size On Disk	Fileset File Count	Policy Name
GLOBAL	80.00 GB	0.00 bytes	0.00 bytes	0	0.00 bytes	0.00 bytes	0	Default Policy
KDANG-015150	80.00 GB	0.00 bytes	0.00 bytes	0	0.00 bytes	0.00 bytes	0	Default Policy
SONICWAL-FFKFVQ	80.00 GB	0.00 bytes	0.00 bytes	0	0.00 bytes	0.00 bytes	0	Default Policy
TELLAKULA-01206	80.00 GB	178.98 MB	174.64 MB	9	0.00 bytes	0.00 bytes	0	Default Policy
VM-VISTA-BUS-02	80.00 GB	9.89 GB	9.90 GB	3	0.00 bytes	0.00 bytes	0	Default Policy
W2K3SBS-001	80.00 GB	39.58 GB	39.60 GB	9	0.00 bytes	0.00 bytes	0	Default Policy
W2K8EE-01	80.00 GB	38.08 GB	25.95 GB	200008	0.00 bytes	0.00 bytes	0	Default Policy
WIN7-02	80.00 GB	45.48 GB	44.83 GB	1001955	0.00 bytes	0.00 bytes	0	Default Policy

- **Disk Space by File Type**

Disk Space by File Type Table

File Type	File Count	Total Size	Total Size On Disk	File Count Percentage(%)	Total Size Percentage(%)	Total Size On Disk Percentage(%)
.tar	1	40.55 MB	40.51 MB	0.00	0.03	0.03
.txt	1200940	14.30 GB	1.47 GB	99.91	10.73	1.22
.zip	1	9.90 GB	9.90 GB	0.00	7.43	8.22
.exe	7	138.43 MB	134.13 MB	0.00	0.10	0.11
EMPTY	1011	0.00 bytes	313.06 KB	0.08	0.00	0.00
.rar	22	108.84 GB	108.90 GB	0.00	81.71	90.41
.bat	2	1.19 KB	623.00 bytes	0.00	0.00	0.00

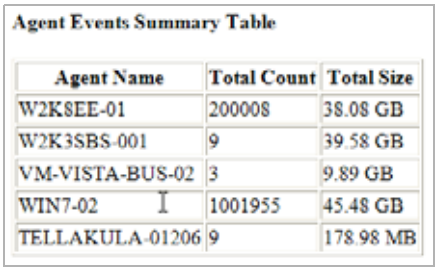
- **Disk Space Summary**



Disk Space Summary Table

Agent Name	Quota	Quota Used	File Count	Offsite Quota	Offsite Quota Used
GLOBAL	80.00 GB	0.00 bytes	0	0.00 bytes	0.00 bytes
KDANG-015150	80.00 GB	0.00 bytes	0	0.00 bytes	0.00 bytes
SONICWAL-FFKFVQ	80.00 GB	0.00 bytes	0	0.00 bytes	0.00 bytes
TELLAKULA-01206	80.00 GB	178.98 MB	9	0.00 bytes	0.00 bytes
VM-VISTA-BUS-02	80.00 GB	9.89 GB	3	0.00 bytes	0.00 bytes
W2K3SBS-001	80.00 GB	39.58 GB	9	0.00 bytes	0.00 bytes
W2K8EE-01	80.00 GB	38.08 GB	200008	0.00 bytes	0.00 bytes
WIN7-02	80.00 GB	45.48 GB	1001955	0.00 bytes	0.00 bytes

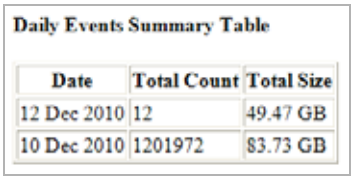
- **Detailed Event List**
- **Agent Event Summary**



Agent Events Summary Table

Agent Name	Total Count	Total Size
W2K8EE-01	200008	38.08 GB
W2K3SBS-001	9	39.58 GB
VM-VISTA-BUS-02	3	9.89 GB
WIN7-02	1001955	45.48 GB
TELLAKULA-01206	9	178.98 MB

- **Daily Events Summary**



Daily Events Summary Table

Date	Total Count	Total Size
12 Dec 2010	12	49.47 GB
10 Dec 2010	1201972	83.73 GB

Step 5 Click **Apply**.

Adding a SonicWALL CDP Appliance to GMS

SonicWALL CDP appliances must be running firmware version 2.3 or later to be managed using SonicWALL Global Management System (GMS). For CDP Reporting in SonicWALL GMS, a minimum of SonicWALL CDP 6.0 is required with SonicWALL GMS 6.0.2 (6.0 Service Pack 2). To configure a SonicWALL CDP appliance for management by SonicWALL GMS, perform the following tasks:

- "Preparing the SonicWALL CDP Appliance" on page 50
- "Adding the SonicWALL CDP Appliance to GMS" on page 51
- "Registration Tasks on GMS" on page 51
- "Registration Tasks on the CDP Appliance" on page 52

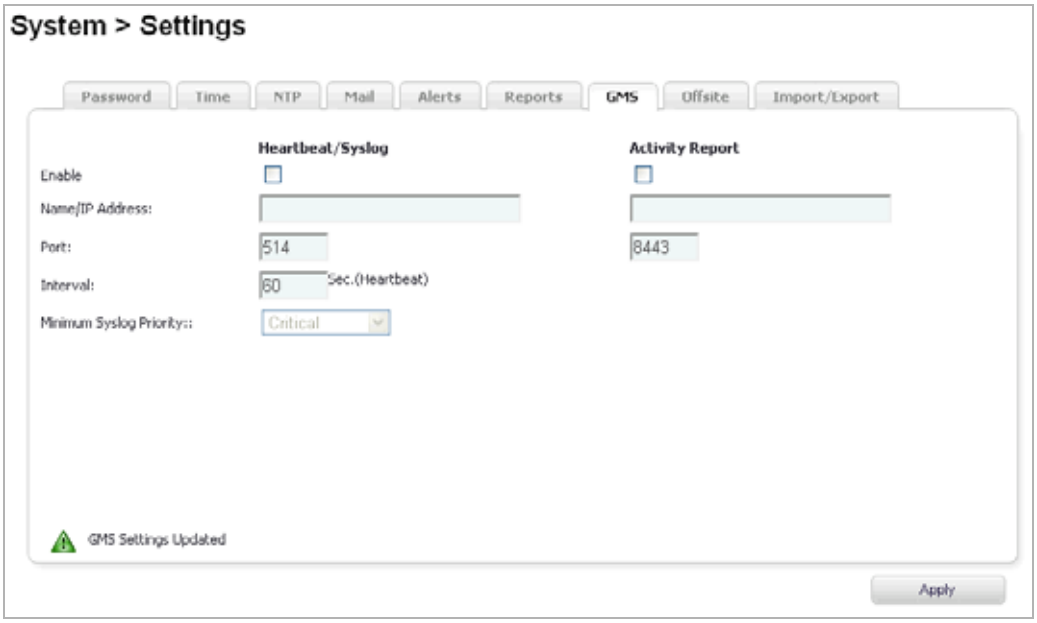
Preparing the SonicWALL CDP Appliance

You can manage the SonicWALL CDP appliance from SonicWALL GMS. The System > GMS page provides a way to add the SonicWALL GMS host name or IP address, and to specify the number of seconds between heartbeats sent to the SonicWALL GMS system.

For more information about adding the appliance to SonicWALL GMS management, see "Adding the SonicWALL CDP Appliance to GMS" on page 51.

To prepare the SonicWALL CDP appliance for GMS management:

Step 1 On the **System > GMS** page, type the GMS host name or IP address of the GMS server and the port number in the **GMS Host Name or IP Address** field. The default port is 514.



Step 2 Under **Heartbeat/Syslog**, select the **Enable** checkbox to enable the CDP appliance to send periodic heartbeats to SonicWALL GMS, and to enable the CDP to send syslog message to GMS.

Step 3 In the **Name/IP Address** field, type the FQDN or IP address of the SonicWALL GMS system.

Step 4 In the **Port** field, enter the port number to be used when sending heartbeats or syslog messages.

Step 5 In the **Interval** field, enter the heartbeat interval, in seconds, . The maximum heartbeat interval is 86400 (24 hours).

Step 6 In the **Minimal Syslog Priority** drop-down list, select one of the following:

- **Critical** – Only send critical syslog messages
- **Warning** – Send critical and warning syslog messages
- **Informational** – Send all syslog messages

Step 7 Under **Activity Report**, select the **Enable** checkbox to enable the CDP appliance to send periodic activity reports to SonicWALL GMS.

Step 8 In the **Name/IP Address** field, type the FQDN or IP address of the SonicWALL GMS system.

Step 9 In the **Port** field, enter the port number to be used when sending activity reports.

Step 10 Click **Apply**.

Adding the SonicWALL CDP Appliance to GMS

To add your appliance to GMS, perform the following tasks:

Step 1 Log in to GMS.

Step 2 Click the **CDP** appliance tab . If the **CDP** appliance tab is not visible above the TreeControl pane, click the down arrow button and select **CDPs** from the drop-down list.

Step 3 In the left-most pane, right click and select **Add Unit**. The Add Unit popup displays.

Step 4 Enter a descriptive name for the SonicWALL appliance in the **Unit Name** field.

Step 5 Enter the appliance administrator login name in the **Login Name** field.

Step 6 Enter the appliance administrator password in the **Password** field.

Step 7 Enter the appliance serial number in the **Serial Number** field. The serial number can be found in the CDP appliance management interface under **General > Status**.

Step 8 The management mode defaults to **Using HTTPS**.

Step 9 Click **OK**.

It may take up to a minute for the data to load.

The SonicWALL CDP is displayed in the left pane of the SonicWALL CDP interface as a yellow icon, which means the unit has not been acquired by SonicWALL GMS. After the appliance has been acquired, the icon will either turn red, indicating that the appliance status is down, or blue, indicating that the appliance status is up.

It may take up to five minutes for the SonicWALL CDP to establish an HTTPS connection and acquire the SonicWALL appliance for management.

Your CDP is now ready for management using SonicWALL GMS.

To register a CDP appliance, you must perform tasks on GMS and on the CDP appliance through its local user interface. See the following sections:

- “Registration Tasks on GMS” section on page 51
- “Registration Tasks on the CDP Appliance” section on page 52

Registration Tasks on GMS

When a unit is added to GMS, once it is acquired successfully by GMS, it is automatically registered by GMS. However, CDP appliances cannot be used until you complete the registration tasks on the local CDP appliance.

You can also register CDP appliances manually in GMS. To register a CDP appliance:

Step 1 In the left pane, select the CDP appliance.

Step 2 Click the **Policies** tab.

Step 3 In the center pane, navigate to **Register/Upgrades > Register CDPs**.

Step 4 Click **Register**. The scheduler displays.

Step 5 Expand the Scheduler settings by clicking the plus button.

Step 6 Do one of the following:

- Select **Immediate**.
- Select the **At** button and specify a date and time for SonicWALL GMS to perform the registration.

Step 7 Click **Accept**.

Note It may take several seconds for GMS to contact MySonicWALL to register the CDP.

Registration Tasks on the CDP Appliance

After the GMS registration completes, you can perform the local registration tasks on the CDP appliance. For more information on CDP registration, see the *SonicWALL CDP Getting Started Guide* for your CDP appliance.

To perform local CDP registration tasks:

Step 1 In GMS, in the left pane, select the CDP unit.

Step 2 Navigate to **Policies > General > Status**.

Step 3 In the right pane, locate the **Registration Code** for use on the local CDP appliance.

Step 4 On the management system for the CDP appliance, point your browser to the SonicWALL CDP Web Management Interface and log in with the default credentials, admin/password.

Step 5 Navigate to the **System > Registration/Licenses** screen.

Step 6 On the **Registration** tab, enter the Registration Code obtained from GMS in the **Registration Code** field.

Step 7 Click the **Register** button.

Configuring the Offsite Service

The procedure for configuring the downstream CDP appliance to back up data and policy information to the SonicWALL CDP Portal or to an upstream CDP appliance is provided in this section.

For information about restoring files from an offsite CDP appliance, see the "Restoring Data from Offsite" section on page 57.

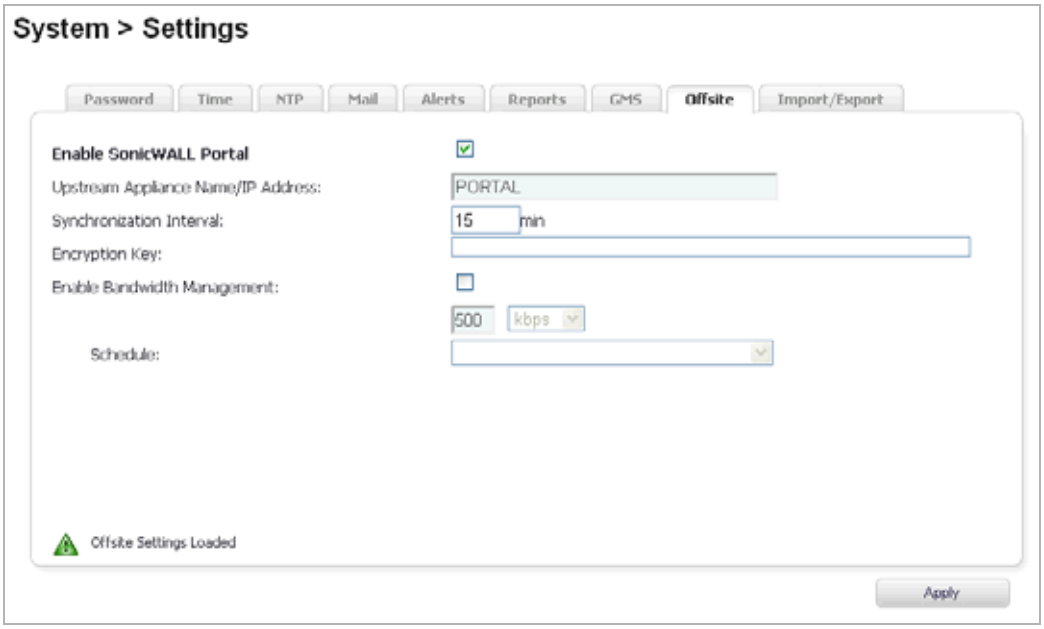
For information about managing and restoring data from an offsite CDP appliance by using the Agent User Interface as an administrator, see the "Using the Agent UI as Administrator" section on page 96.

For more detailed information about the SonicWALL CDP Offsite and Site-to-Site Backup and Restore feature, see the "Site-to-Site Service Overview" on page 201 and subsequent sections.

To configure the downstream CDP appliance to back up to the SonicWALL CDP Portal or to an upstream CDP appliance, perform the following steps:

Step 1 Login to the downstream CDP appliance using the Web Management Interface.

Step 2 Navigate to the **System > Settings** page and select the **Offsite** tab.



Step 3 To use the SonicWALL Portal as the upstream destination, leave the **Enable SonicWALL Portal** checkbox selected and leave **PORTAL** in the **Upstream Appliance Name/IP Address** field.

Step 4 To use another SonicWALL CDP appliance as the upstream destination, clear the checkbox next to **Enable SonicWALL Portal** and type the IP address or the FQDN (Fully Qualified Domain Name) of the upstream CDP appliance in the **Upstream Appliance Name/IP Address** field.

Note It is important that the upstream and downstream appliances have different IP addresses. Refer to the *SonicWALL CDP Getting Started Guide* for further information on configuring an appliance's IP address and domain name.

Step 5 Set the desired number of minutes in the **Synchronization Interval** field. The default, and minimum, is 15 minutes. To save bandwidth, you can set the interval to a larger number for less frequent synchronization between the downstream and upstream appliances..

Step 6 The **Encryption Key** is set automatically, and cannot be changed. If you switch between the Portal and another upstream destination, you will see a different key in this field. You can copy the key to your computer clipboard and save it in a text file for secure storage offsite.

Step 7 To specify the maximum bandwidth used during synchronization with the upstream destination, select the **Enable Bandwidth Management** checkbox, enter the desired numerical value in the field below it, and select **kbps**, **Mbps**, or **Gbps** as the units.

Step 8 To enforce a schedule for synchronization with the upstream destination, select the **Enable Bandwidth Management** checkbox and then select the desired schedule from the **Schedule** drop-down list. You can configure an appropriate schedule on the **Policy > Schedules** page.

Step 9 Click **Apply**.

Exporting or Importing Preferences

You can export or import preferences (system and policy configuration settings) on the **Import/Export** tab of the System > Settings page. Exporting preferences saves all configuration data to an encrypted file.

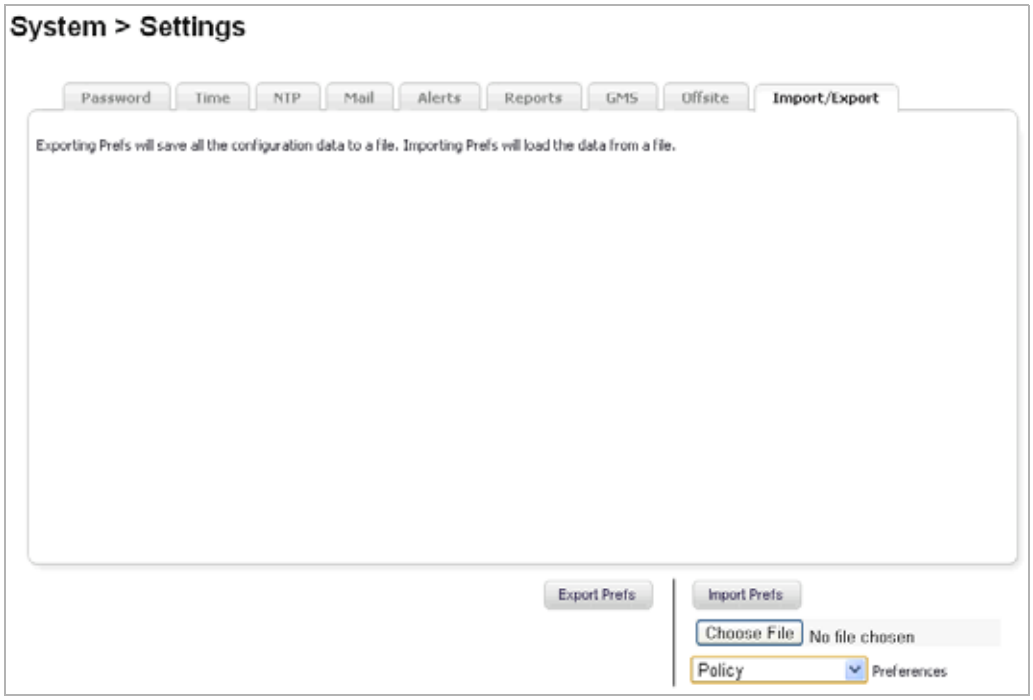
Importing preferences loads the data from a file that you choose. When importing, you can select the type of settings to import:

- **Policy** – Import all policy configuration settings
- **System** – Import all system configuration settings
- **Policy and System** – Import all settings

Exporting Preferences

To export preferences:

Step 1 Navigate to the **System > Settings** page and click the **Import/Export** tab.



Step 2 Click the **Export Prefs** button.

The preferences are downloaded to the ***prefs.txt*** file. The file is placed in your default downloads folder, such as *...\My Documents\Downloads*. The content is encrypted to prevent unauthorized access.

Importing Preferences

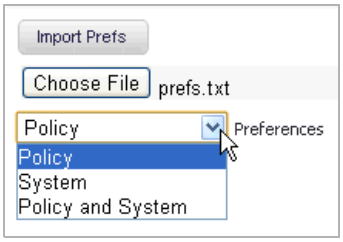
To import preferences:

Step 1 Navigate to the **System > Settings** page and click the **Import/Export** tab.

Step 2 Click the **Choose File** button and browse to the desired prefs file and select it.

The file name appears next to the **Choose File** button.

Step 3 Select the type of preferences to import from the Preferences drop-down list.



You can select one of the following:

- **Policy** – Import all policy configuration settings
- **System** – Import all system configuration settings
- **Policy and System** – Import all settings

Step 4 Click the **Import Prefs** button.

Step 5 Click **OK** in the dialog box that is displayed when the import completes.

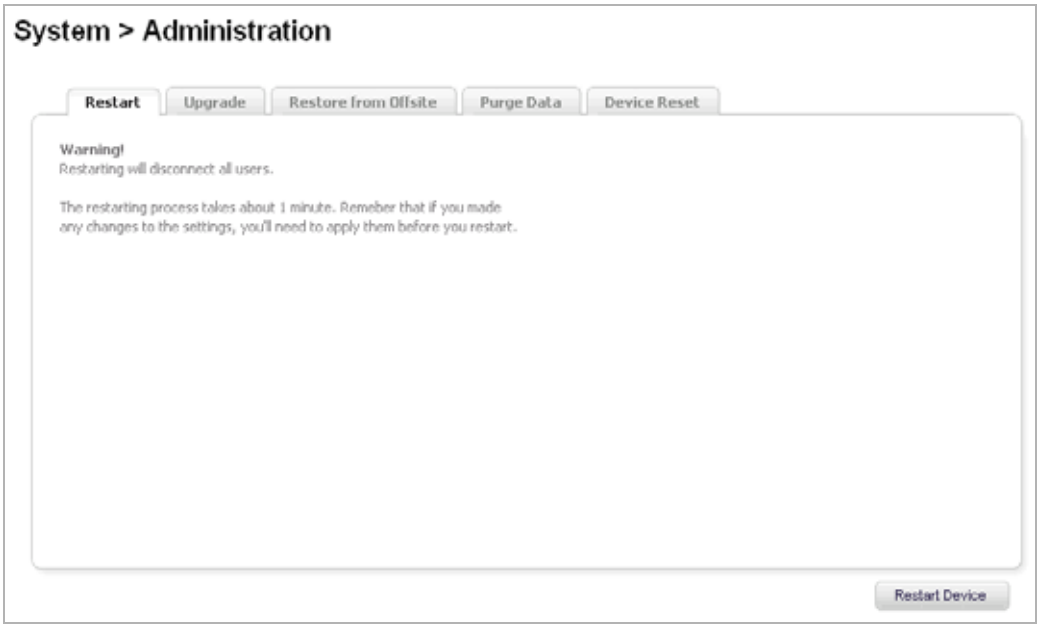
Administrative System Tasks and Settings

The System > Administration page provides several administrative functions, including restarting and upgrading the SonicWALL CDP appliance. Administrators are able to purge data and reset the SonicWALL CDP appliance to factory defaults.

Restarting the Appliance

To restart the SonicWALL CDP appliance, perform the following steps:

Step 1 Navigate to the **System > Administration** page and select the **Restart** tab.


System > Administration
Restart
Upgrade
Restore from Offsite
Purge Data
Device Reset
Warning!
Restarting will disconnect all users.
The restarting process takes about 1 minute. Remeber that if you made
any changes to the settings, you'll need to apply them before you restart.
Restart Device

Step 2 Verify that any updated settings have been applied.

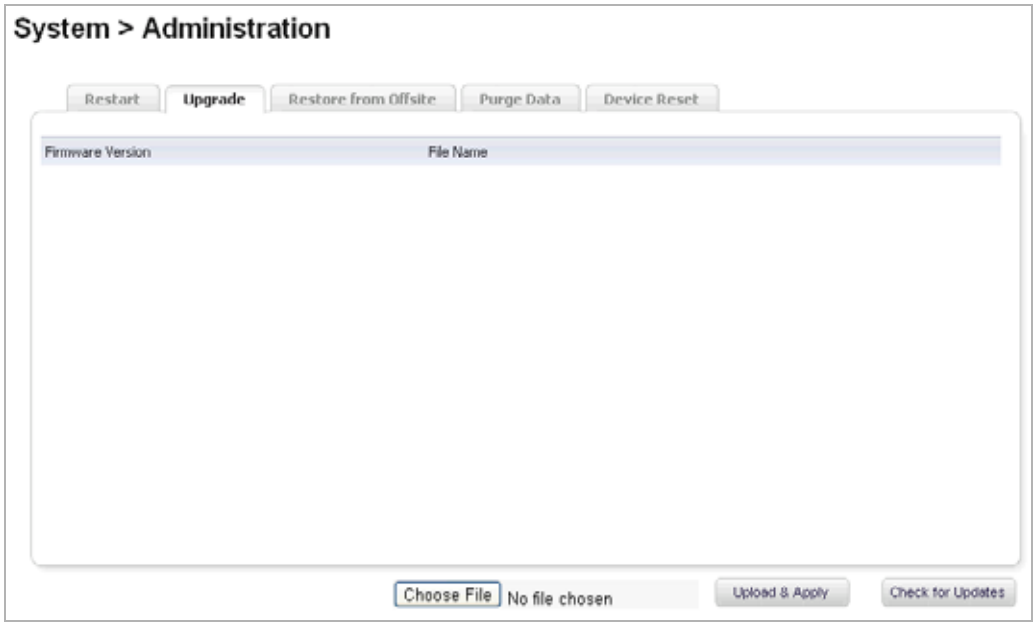
Step 3 Click the **Restart Device** button.

Restarting the appliance disconnects all users and agents.

Upgrading Appliance Firmware

To upgrade the firmware on the SonicWALL CDP appliance, perform the following steps:

Step 1 Navigate to the **System > Administration** page and select the **Upgrade** tab.



Step 2 Click the **Check for Updates** button. If any new firmware versions are available for download on MySonicWALL, the versions will appear on the page.

Step 3 Click the **Choose File** button and browse to select the downloaded firmware file to use.

Step 4 Click **Upload & Apply** to upload the chosen file to the appliance and then reboot the appliance using the new firmware.

Step 5 Click **OK** in the confirmation dialog.

Purging Data from the SonicWALL CDP Appliance

In the event that your appliance is damaged and needs to be returned to SonicWALL, you may want to purge its contents, including stored data and agent information.

Caution Purge data erases all backed up data on the appliance. It is impossible to recover the data once it is purged. Purging the data does not change IP or password settings.

To purge data from the SonicWALL CDP appliance, perform the following steps:

Step 1 Navigate to the **System > Administration** page and select the **Purge Data** tab.

System > Administration
Restart
Upgrade
Restore from Offsite
Purge Data
Device Reset
Warning! This operation will irrevocably destroy all backed up data on this appliance.
It will be impossible to recover the data. Are you absolutely sure you want to proceed?
Purge Data

Step 2 Click **Purge Data**.

Step 3 Click **Yes - Purge Now** to confirm and purge backup data.

Step 4 A confirmation message displays upon completion of the data purge.

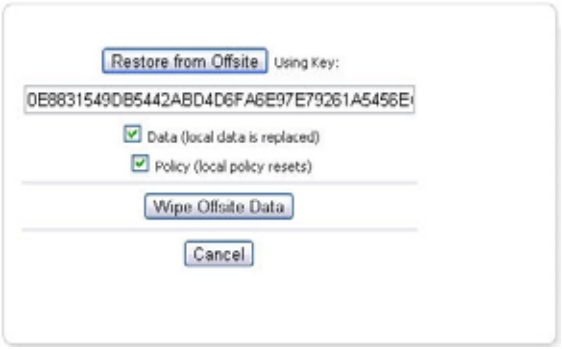
Restoring Data from Offsite

The procedure for restoring data and policy information from the SonicWALL CDP Portal or from an upstream CDP appliance is provided in this section. For more detailed information about the SonicWALL CDP Offsite and Site-to-Site Backup and Restore service, see the "Site-to-Site Service Overview" on page 201 and subsequent sections.

To restore data and policy information from the upstream appliance to the downstream appliance, perform the following steps:

Step 1 Login to the downstream CDP appliance using the Web Management Interface.

Step 2 Navigate to the **System > Administration** page and click the **Restore from Offsite** tab.



Step 3 If a new downstream appliance is set up, verify that the correct key is in the key field.

Step 4 To restore data, select the **Data** checkbox.

Step 5 To restore settings and configurations, select the **Policy** checkbox.

Note Once the old appliance's settings and configurations are downloaded after selecting the **Policy** checkbox, the new appliance will begin backing up the local agents immediately. It may not be necessary to download the old data from the upstream appliance.

Step 6 Click **Restore from Offsite**.

Step 7 A warning message displays. Click **Yes** to continue.

Note The data on the downstream appliance will be replaced with the data from the upstream appliance.

Step 8 A second warning message displays. Click **Yes** to continue.

Note The data restore process cannot be canceled once it has started.

The restore progress displays. Click **Close** to close the progress page.

Resetting to Factory Defaults

You can reset the SonicWALL CDP appliance to factory default settings on the **Device Reset** tab on the System > Administration page. Resetting the appliance to factory default settings will remove all data, as well as all configuration settings and will reboot the appliance. After a device reset, you must use the default credentials, admin/password, to login.

To reset the appliance to factory defaults:

Step 1 Navigate to the **System > Administration** page and click the **Device Reset** tab.

System > Administration
Restart
Upgrade
Restore from Offsite
Purge Data
Device Reset
Warning! Resetting appliance to factory default settings will remove all data as well as all configuration settings and reboot the appliance.
Reset Device

Step 2 Click **Reset Device**.

Step 3 In the confirmation page, click **Yes** to reset the appliance to factory defaults.

System Diagnostics

The Web management interface provides five diagnostics displays for the SonicWALL CDP appliance on the System > Diagnostics page:

- CPU information, including vendor ID, model, cache size, MHz, and many characteristics
- Memory usage, including free memory, buffers in use, cached, active, inactive, swap usage, mapped pages, and other data
- Network information, including link status, packet count, and other data for eth0 and eth1, and also displays active Internet connections with local and foreign addresses, and information about active UNIX domain sockets
- System processes, including user ID, process ID, PPID, time, command, and other data

- Storage statistics, including file system name, total file system capacity, disk space used, disk space available, percentage of space used, and the directory name where the file system is mounted

System Licenses and Registration

The System Licenses and Registration page displays details about the license and registration status of security services and supported services.

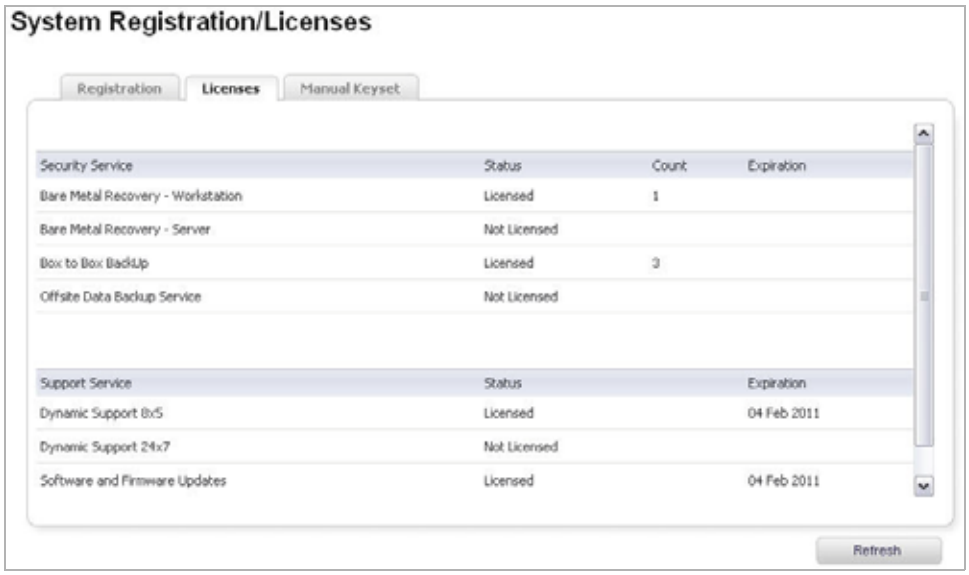
For the registration procedure, see the “Registering the SonicWALL CDP Appliance” section on page 31.

Registration Status

The Registration tab displays the current registration status of the SonicWALL CDP appliance.

Licenses

Click the **Refresh** button to update the page after subscribing to a service on MySonicWALL.



Manual Keyset

This feature allows you to fetch licenses (bypassing Web Management Interface registration), if your SonicWALL CDP appliance is deployed in an environment that does not allow direct or reliable Internet connectivity from the SonicWALL appliance.

To acquire the license:

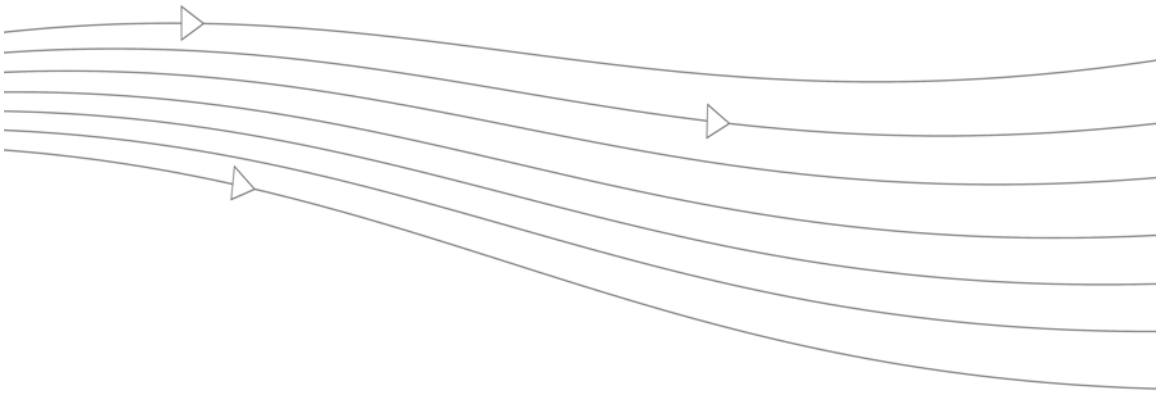
Step 1 Obtain the encrypted license key information from your mysonicwall.com account for the SonicWALL CDP appliance by clicking on the “View License Keyset” link.

Step 2 Copy the license to the Manual Keyset field on the System > Licenses page.

Note This feature is only available for CDP users who have a mysonicwall.com account.

System Activity Progress

The System > Activity Progress page displays status information about data transfer to the offsite portal or device. If no activity is occurring, the Status is displayed as Idle.



Chapter 4: Configuring Network Settings

The Network pages provide configuration options for the SonicWALL CDP appliance IP address, subnet mask, default gateway IP address and interface, name servers, hostname and domain. You can also test network and security connectivity.

See the following sections:

- "Network Interface Overview" section on page 63
- "Configuring Network Settings" section on page 64
- "Testing Network Connectivity" section on page 66

Network Interface Overview

The Network Interface allows you to configure network settings for the SonicWALL CDP Appliance.

Network Options	Description
Settings	Provides access to configuration options, including IP address, subnet mask, default gateway IP address and interface, name servers, and hostname and domain.
Connectivity	Provides access to options for testing connectivity, including pinging the registration server, pinging a URL and resolving a URL.

Configuring Network Settings

The Network > Settings page allows you to configure your SonicWALL CDP appliance to communicate with your network.

Note For initial setup of your SonicWALL CDP appliance, see the *SonicWALL CDP Getting Started Guide* for your model.

This section contains the following subsections:

- "Configuring Appliance Host Name and Domain" section on page 64
- "Configuring IP, Subnet, and Gateway Addresses" section on page 65
- "Configuring the Domain Name Server Address" section on page 66

Configuring Appliance Host Name and Domain

The Summary tab located on the **Networks > Settings** page allows the administrator to configure the host name, domain, and friendly name for the SonicWALL CDP appliance.

Step 1 Point the browser on your management computer to the SonicWALL CDP Web Management Interface and navigate to **Network > Settings** in the left-hand menu and select the **Summary** tab.

Step 2 Type the host name for the SonicWALL CDP appliance into the **Name** field.

Step 3 Type the domain name for the appliance into the **Domain** field.

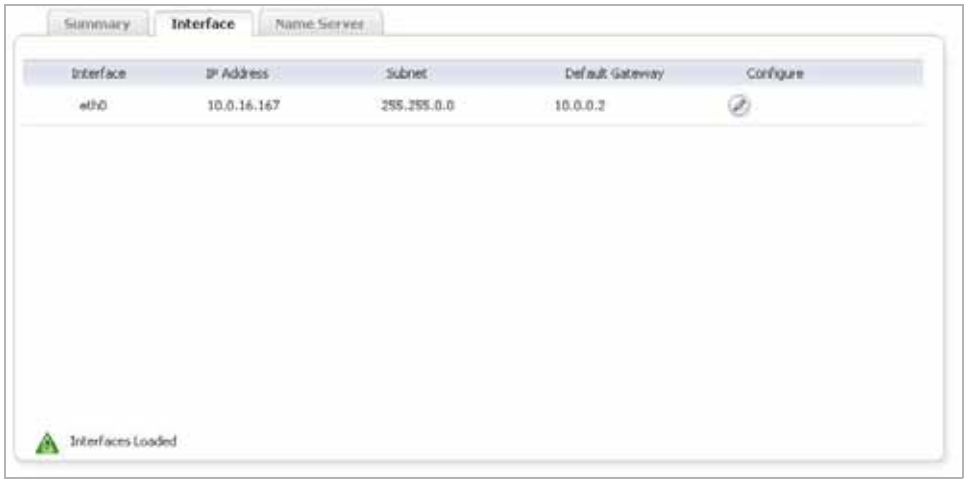
Step 4 Type a descriptive name for the appliance into the **Friendly Name** field.

Step 5 Click the **Apply** button.

Configuring IP, Subnet, and Gateway Addresses

The Interface tab located on the **Networks > Settings** page allows the administrator to configure the IP address, subnet address, and gateway address for the SonicWALL CDP appliance.

Step 1 Navigate to **Network > Settings** in the left-hand menu. Select the **Interface** tab and click the **Configure** icon in the table.



Step 2 Specify a name for the interface in the **iface** field.

Step 3 Specify the IP Address in the **ip** field by entering an unused static IP address within range of your local subnet.

Step 4 Enter your subnet mask in the **netmask** field.

Using an IP address within the range of a local subnet is accomplished by keeping the network portion, according to the subnet mask, of the LAN gateway IP address the same. For example, if your gateway IP address is **10.10.10.1** and your subnet mask is **255.255.255.0**, you can set your SonicWALL CDP appliance IP address to **10.10.10.20**.

Step 5 Enter the default gateway address in the **gateway** field. The gateway is typically a firewall in your subnet that also has access to the Internet.

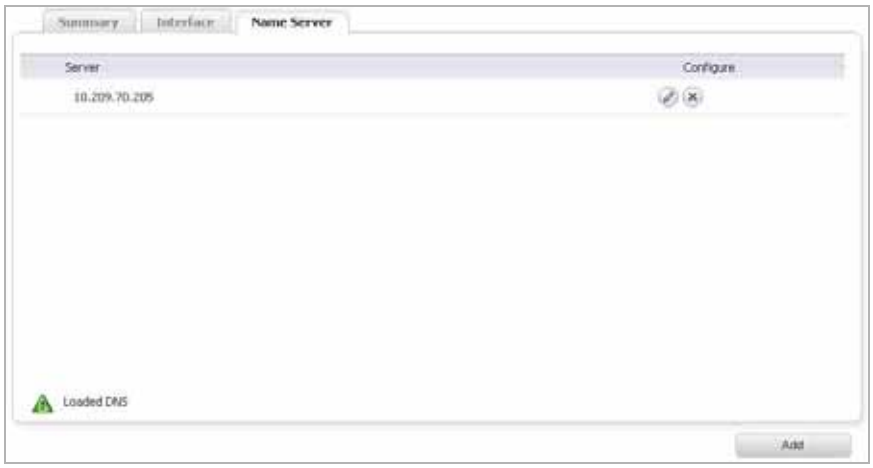
Step 6 Click **Save**.

Note You may lose connectivity with the SonicWALL CDP appliance during an IP address change. This occurs because the SonicWALL CDP appliance is now on a different subnet than the management computer. To reconnect, point your browser to the new IP address (http://<new IP address>).

Configuring the Domain Name Server Address

You must configure the correct Domain Name Server (DNS) address settings in order to register and use your SonicWALL CDP appliance. The DNS must be able to resolve external Internet names.

Step 1 Navigate to **Network > Settings** in the left-hand menu. Select the **Name Server** tab.



Step 2 Click the **Add** button located in the lower-right, below the Name Server table.

Step 3 Enter a single Domain Name Server in the **server** field and click **Save**. Repeat steps 2 and 3 to add additional DNS entries if more DNS entries are desired.

New Domain Name Servers are now available in the Server list. To remove a domain name server, click the **X** button next to the server.

Testing Network Connectivity

You can test the network connectivity, trace routes, test connectivity to a certain URL, and resolve URLs on the **Network Connectivity** page. For detailed information, see the following sections:

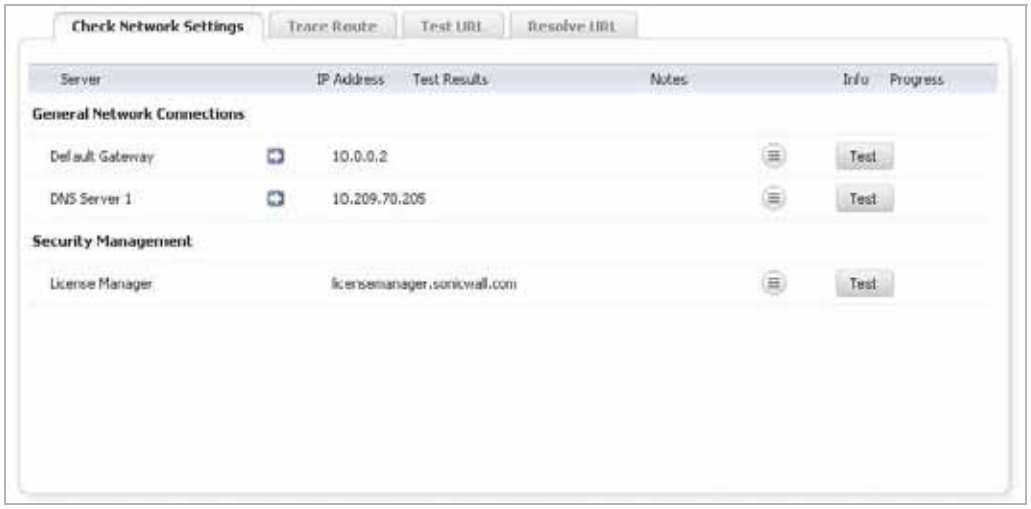
- “Checking Network Settings” section on page 67
- “Tracing Network Routes” section on page 68
- “Testing URL Connectivity” section on page 69
- “Resolving URLs” section on page 70

Checking Network Settings

General network connections such as the default gateway and DNS servers can be tested on the **Check Network Settings** tab. You can also test the connectivity to the SonicWALL license manager.

To check the network connections, perform the following steps:

Step 1 Navigate to **Network > Connectivity** and click on the **Check Network Settings** tab.

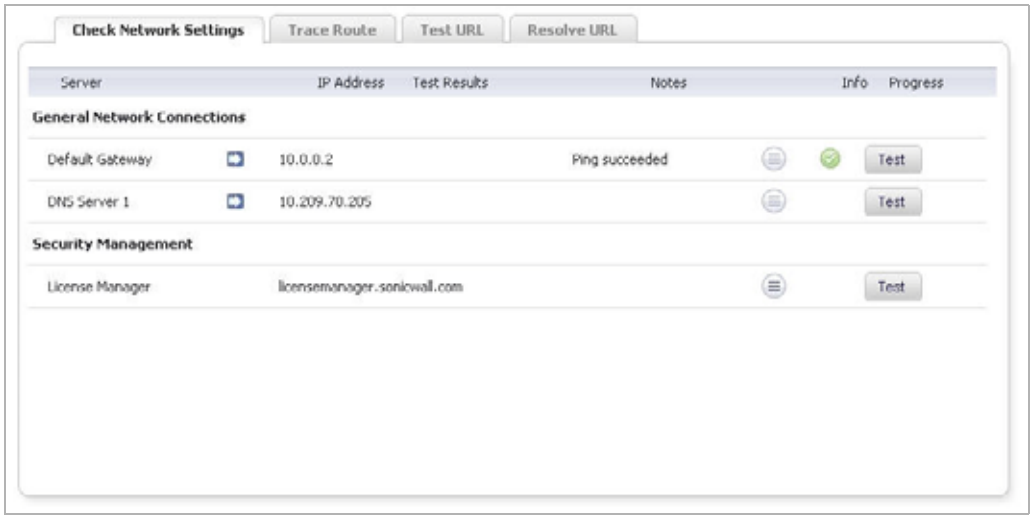


Step 2 Locate the General Network Connection you wish to test. For this example, the Default Gateway is used.

Step 3 Click on the **Test** button located to the right of the desired connection to be tested.

Step 4 The test results column will display the results of the network connection test.

- If the test was successful, **Ping succeeded** is visible.
- If the network connection test failed, **Ping failed** is visible.

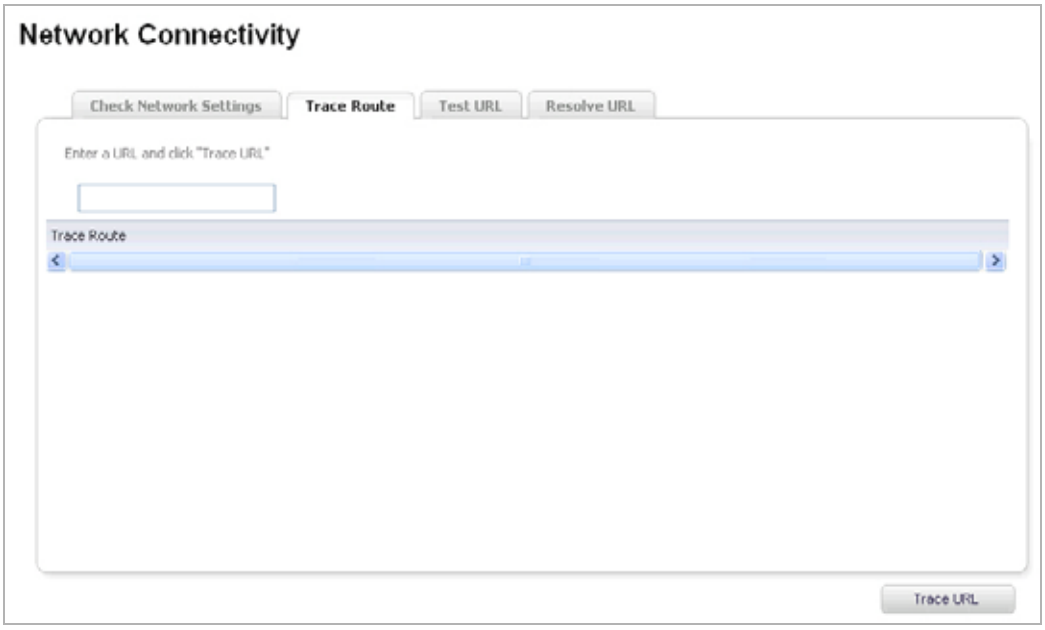


Tracing Network Routes

You can type in a URL on the **Trace Route** tab to find out the network route that traffic from the SonicWALL CDP appliance takes to reach that location.

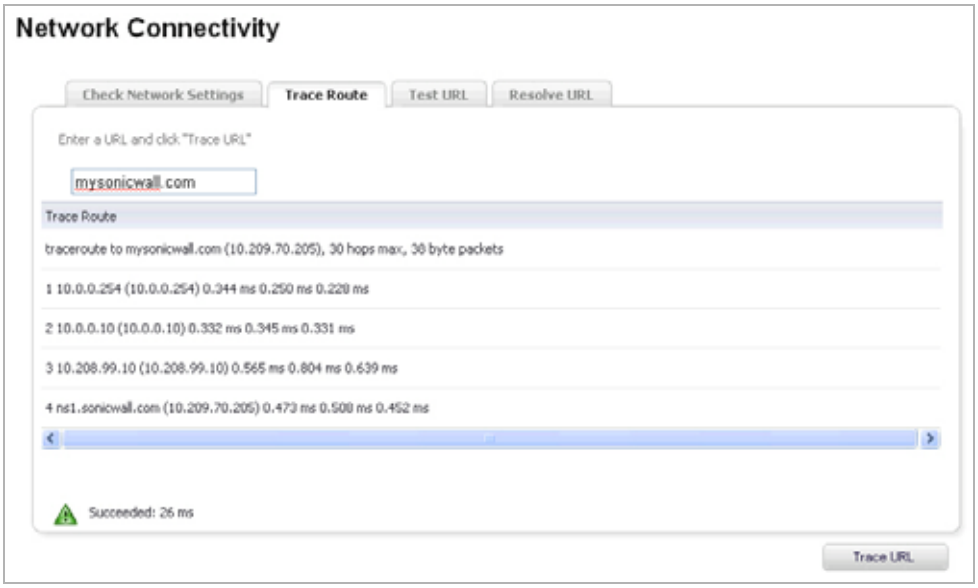
To trace the route to a particular URL, perform the following steps:

Step 1 Navigate to **Network > Connectivity** and click on the **Trace Route** tab.



Step 2 In the text box near the top of the page, type in an IP address or a URL in the form of “mysonicwall.com”.

Step 3 Click the **Trace URL** button. If the trace is successful, the IP address of each hop is displayed, beginning with the network device closest to the SonicWALL CDP and ending with the one closest to the target URL. The status indicator at the bottom of the window displays “Succeeded” and shows the number of milliseconds it took to trace the route.


Network Connectivity
Check Network Settings
Trace Route
Test URL
Resolve URL
Enter a URL and click "Trace URL"
mysonicwall.com
Trace Route
traceroute to mysonicwall.com (10.209.70.205), 30 hops max, 38 byte packets
1 10.0.0.254 (10.0.0.254) 0.344 ms 0.250 ms 0.228 ms
2 10.0.0.10 (10.0.0.10) 0.332 ms 0.345 ms 0.331 ms
3 10.208.99.10 (10.208.99.10) 0.565 ms 0.804 ms 0.639 ms
4 ns1.sonicwall.com (10.209.70.205) 0.473 ms 0.508 ms 0.452 ms
Succeeded: 26 ms
Trace URL

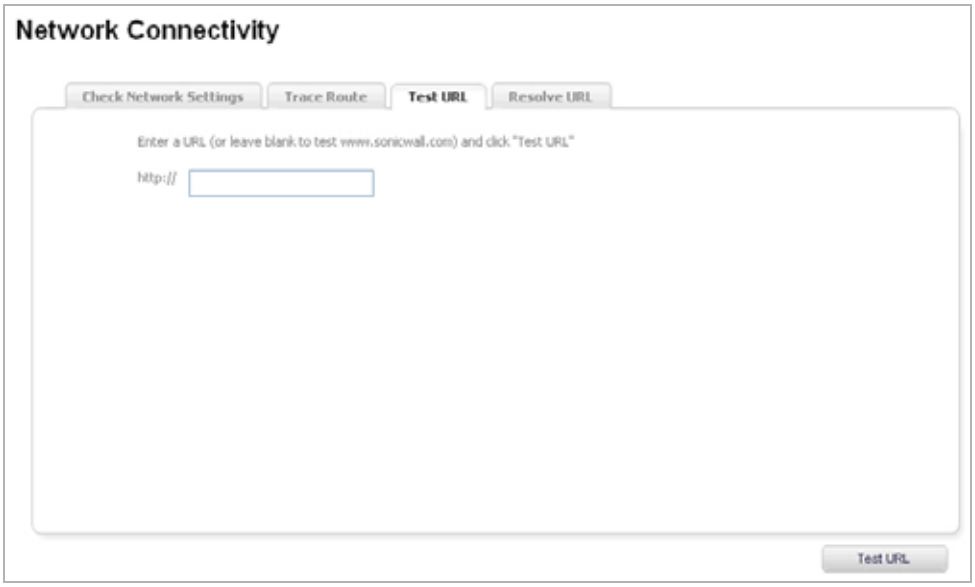
If the URL is unreachable, the status message at the bottom of the window indicates the failure of the trace.

Testing URL Connectivity

You can test the connectivity to a certain URL by typing it in on the **Test URL** tab. If the test succeeds, you know that the SonicWALL CDP appliance can reach that location.

To test the connectivity to a particular URL, perform the following steps:

Step 1 Navigate to **Network > Connectivity** and click on the **Test URL** tab.



Step 2 Type the URL you wish to test into the text field, either as an IP address or in the form “mysonicwall.com”. To test connectivity from the SonicWALL CDP appliance to the default URL, sonicwall.com, you can leave the field blank.

Step 3 Click the **Test URL** button. If the appliance can connect to the URL, the status indicator at the bottom of the window displays “Succeeded” and shows the number of milliseconds it took to connect.

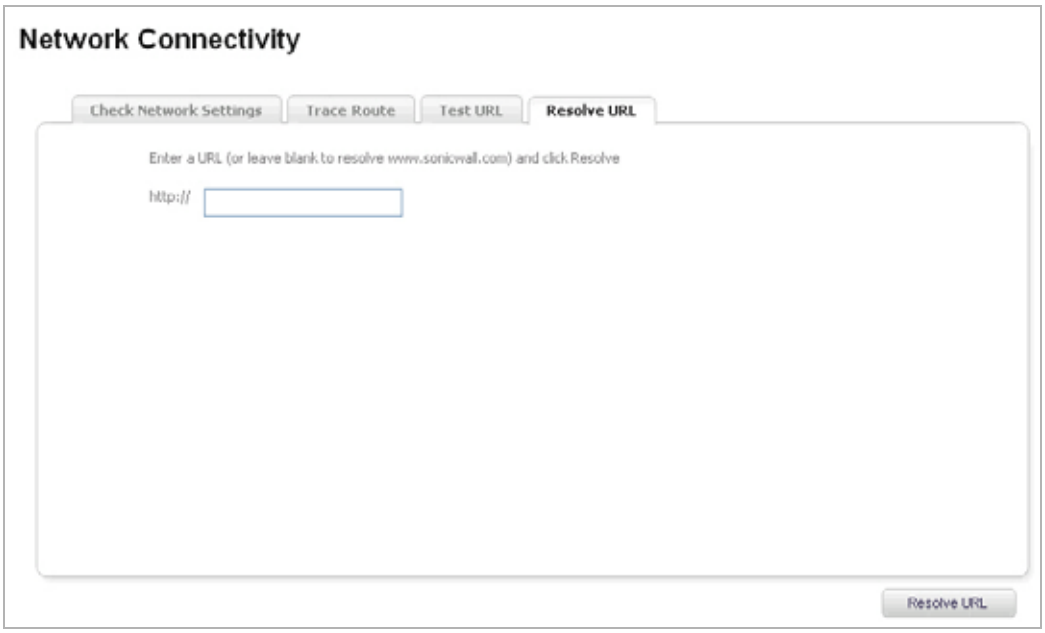
If the appliance cannot connect to the URL, the status indicator displays “failed”.

Resolving URLs

You can resolve a URL to find out its IP address(es) by typing in the URL on the **Resolve URL** tab.

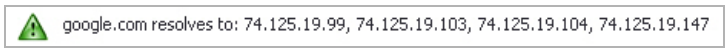
To resolve a URL, perform the following steps:

Step 1 Navigate to **Network > Connectivity** and click on the **Resolve URL** tab.

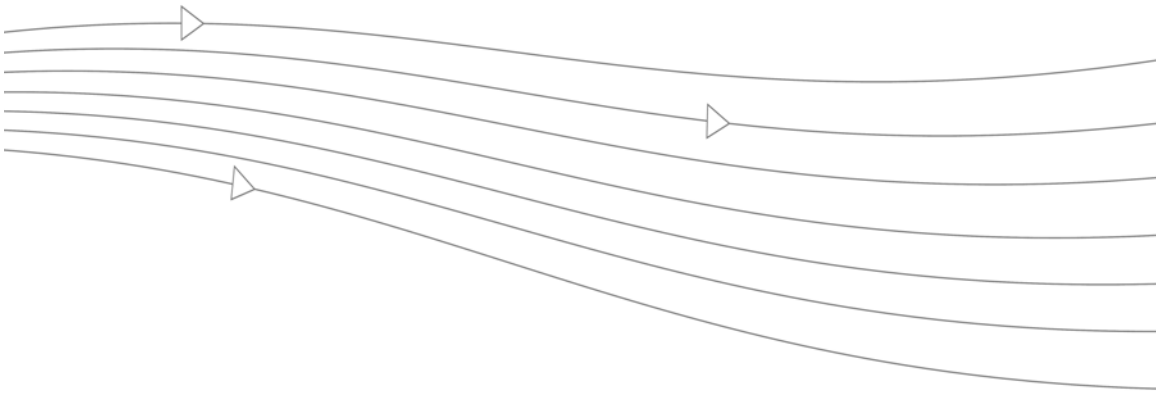


Step 2 Type the URL you wish to resolve into the text field, in the form “mysonicwall.com”. To test connectivity from the SonicWALL CDP appliance to the default URL, sonicwall.com, you can leave the field blank.

Step 3 Click the **Resolve URL** button. If the appliance can resolve the URL, the status indicator at the bottom of the window displays one or more IP addresses for the URL.



If the appliance cannot connect to the URL, the status indicator displays “failed”.



Chapter 5: Creating Files and Folders Backup Policies

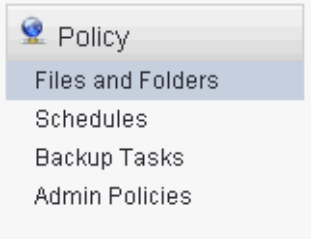
This chapter provides information about the Policies pages in the SonicWALL CDP Web Management Interface, including navigational elements and configuration guidelines. Files and Folders policies are the focus of this chapter; for information about Application policies, see the Backing Up Applications chapter.

This chapter includes the following sections:

- "Policy Interface Overview" section on page 72
- "Creating a Files and Folders Object" section on page 73
- "Creating a Schedule Object" section on page 75
- "Creating a Backup Task Object" section on page 79
- "Creating a Global Policy" section on page 82

Policy Interface Overview

The Policy Interface allows you to define, configure, and implement backup policies for Agents.



Policy Options	Description
Files and Folders	Provides access to create and configure Files and Folders Objects.
Schedules	Provides access to create and configure Schedule Objects
Backup Tasks	Provides access to create and configure Backup Task Objects.
Admin Policies	Provides access to create and implement global and local Policies.

Creating a Files and Folders Object

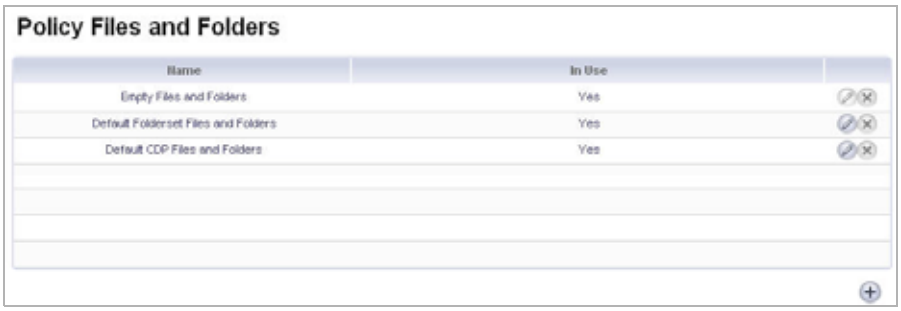
In order to create a Backup Policy, a defined Files and Folder Object, Schedule Object, and Backup Task Object are needed.

By default there are three predefined Files and Folders objects:

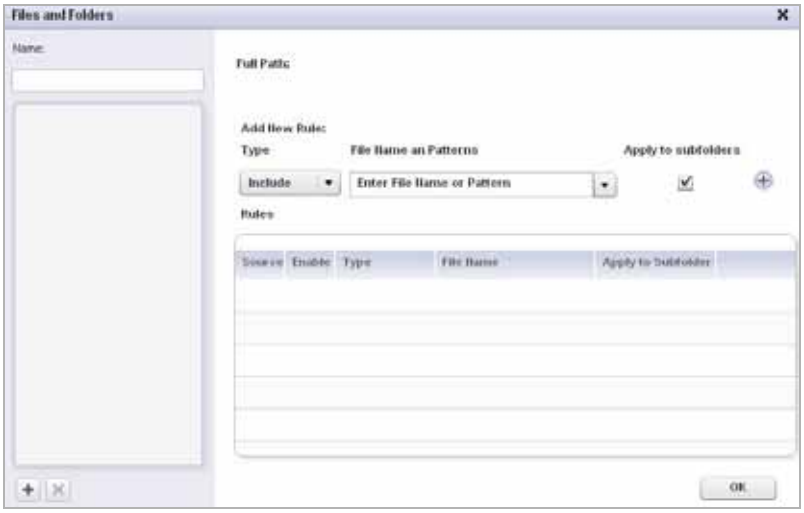
- **Empty Files and Folders** – A non-editable empty Files and Folders object.
- **Default Folderset Files and Folders** – The default object selected in Files and Folders in the Default Policy.
- **Default CDP Files and Folders** – This is the default object selected in the CDP Backup Task in the Default Policy.

To create a Files and Folders Object, perform the following steps:

Step 1 Navigate to **Policy > Files and Folders**.

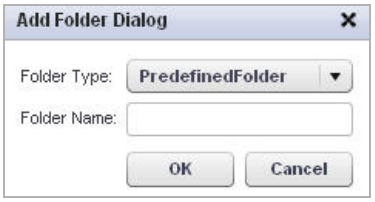


Step 2 Click the **+** button located in the bottom-right below the Files and Folders table. The **Files and Folders** window appears.



Step 3 Specify a friendly name for your Files and Folder Object in the **Name** field.

Step 4 Click the **+** button located in the lower-left corner of the Files and Folders window. The **Add Folder Dialog** appears.



Step 5 Two options are available:

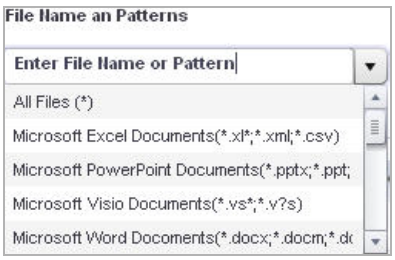
- Select the folder type and click **OK**.
- If **Predefined Folder** is selected, then a complete folder path must be entered. Click **OK**.

Step 6 Define the rules for your Files and Folders Object by first determining how to apply the rule by choosing **Include** or **Exclude** under the **Type** drop-down menu.

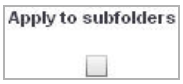
- **Include**: includes the specified files or extensions.
- **Exclude**: excludes the specified files or extensions.

Note The rules are applied in descending order, giving the top rules precedence over rules below. You can change the order of the rules by clicking the up and down arrows in the Rules table.

Step 7 Define the **File Name** by entering a file name, extension, or select from a predefined list.



Step 8 If desired, check the **Apply to Subfolders** check box to apply the rules to subfolders.



Step 9 Click the **+** button to add the rule to the Files and Folders Object. If desired, repeat these steps to create more rules.

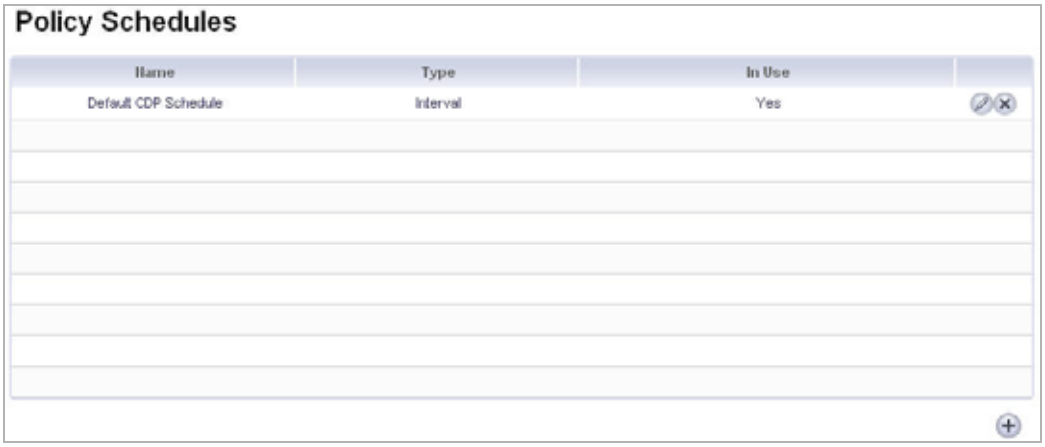
Step 10 Click **OK** after Files and Folders Object creation is complete. New Files and Folder Object(s) are visible in the table.

Creating a Schedule Object

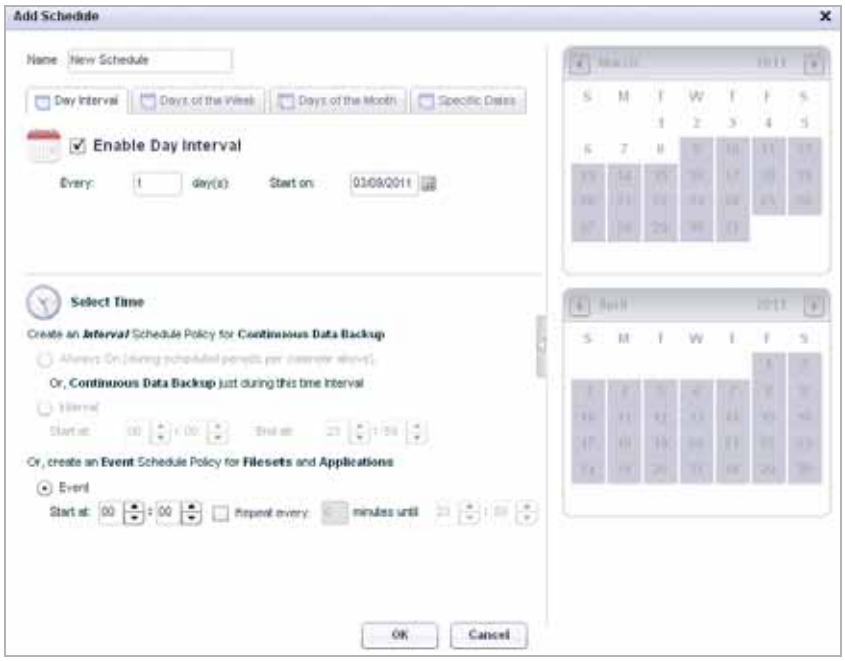
A schedule object defines the exact time and calendar scheduling for when backups occur. The same Schedule object can be used in multiple Backup Tasks.

To create a Schedule object, perform the following steps:

Step 1 Navigate to **Policy > Schedules**.



Step 2 Click the **+** button located in the bottom-right below the Schedule table. An **Add Schedule** window appears.



Step 3 Enter a friendly name for the new Schedule Object in the **Name** field.

Step 4 Specify the type of schedule and time desired. Four options are available and can be combined to form a schedule policy.

1. **Day Interval**: Schedule a task to run every certain number of days calculated from a particular date.

There are two types of schedules:

- **Interval** type of schedule for a CDP type backup task - choose the **Always On** or **Interval** radio button
- **Event** type of schedule for a Fileset or Application backup task - choose the **Event** radio button

– Select the **Enable Day Interval** checkbox.

– Select the number of days for the interval between backups.

– Select a start date. By default, the interval is calculated from the current date.

– Under **Select Time**, select and configure one of the following options:

• To back up the files at any time that a change occurs, select the **Always On** radio button. You can use this type of schedule for a CDP type backup task.

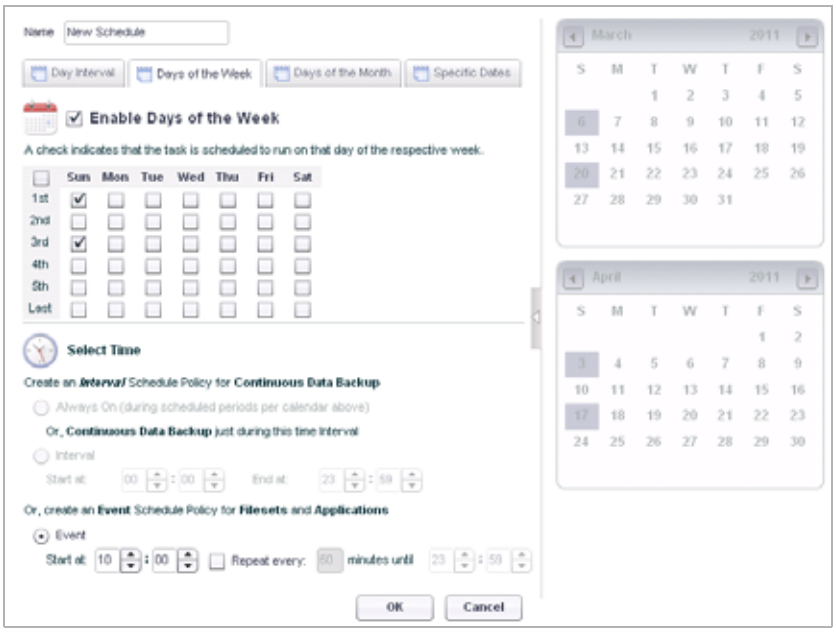
• To back up the files when a change occurs only during a specified time range, select the **Interval** radio button, also for a CDP type backup task, and configure the following:

In the **Start at** fields, the up and down arrows in the left field are used to configure the starting hour, and in the right field to configure the starting minute.

In the **End at** fields, the up and down arrows in the left field are used to configure the ending hour, and in the right field to configure the ending minute.

– To back up the files every certain number of minutes beginning at a specific time, select the **Event** radio button, then fill in the **Start at** fields by selecting an hour and a minute for the start time. Select the **Repeat** checkbox and type a value into the **Repeat every** ... **minutes** field, and select an hour and minute for the end time after **until**. Use Event scheduling for a Fileset or Application backup task.

2. **Days of the week**: Schedule a task to run on a specific day of the respective week.

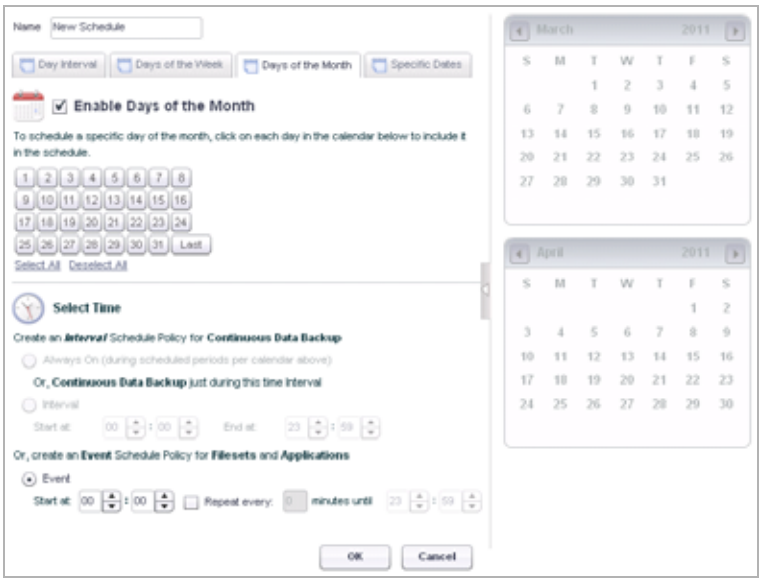


– Select the **Enable Days of the Week** checkbox.

– Select the days of the week, Sunday through Saturday, on which to run the backup.

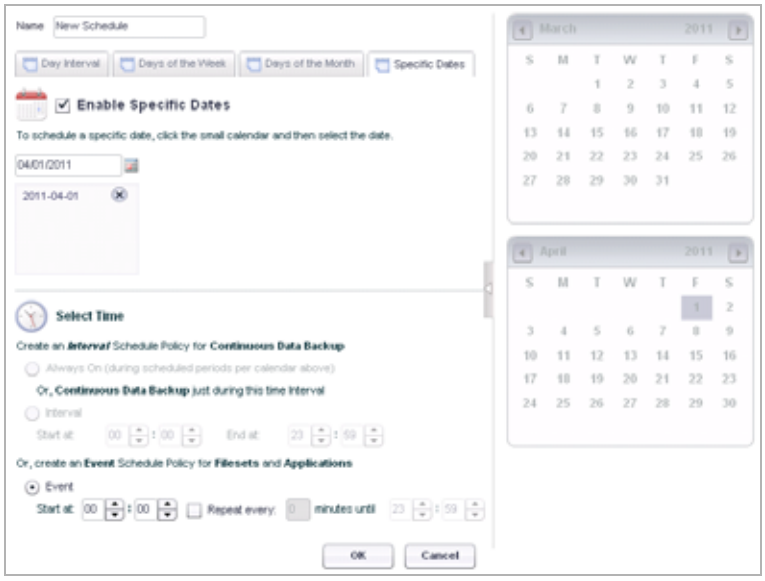
– Select the time at which to start the backup.

3. **Days of the Month**: Schedule a task on a specific day of the month.



- Select the **Enable Days of the Month** checkbox.
- Select the days of the month on which to run the backup. Select **Last** for the last day of the month.
- Select the time at which to start the backup.

4. **Specific Dates**: Schedule a task on specific dates throughout the year.



- Select the **Enable Specific Dates** checkbox.
- Click the small calendar and then select the date(s).
- Select the time at which to start the backup.

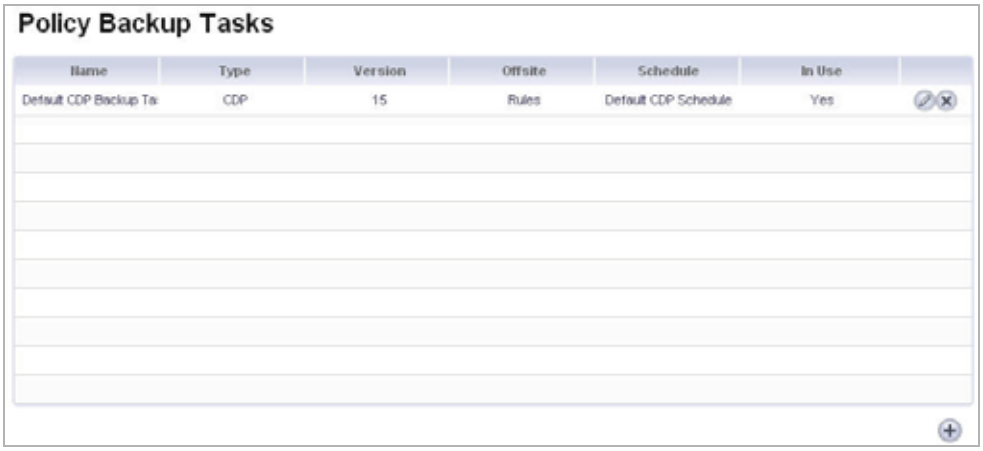
Step 5 Click **OK** after defining the desired schedule. New schedules are visible in the table.

Creating a Backup Task Object

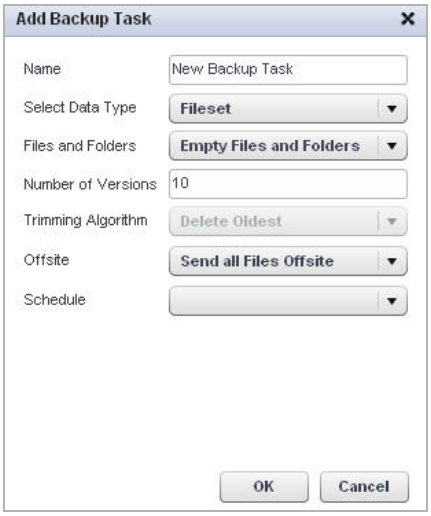
The Backup Task object is created and defined by combining a Schedule object and a File and Folders object, or by combining a Schedule object and an Application object.

To create a Backup Task with a Schedule object and a File and Folders object, perform the following steps:

Step 1 Navigate to **Policy > Backup Task**.



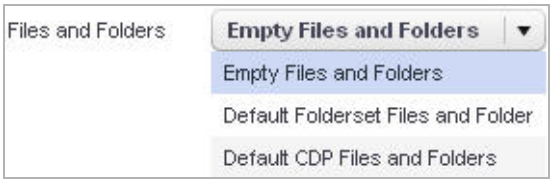
Step 2 Click the **+** button located in the bottom-right, below the Policy Backup Tasks table. An **Add Back Up Task** dialog appears.



Step 3 Define a Backup Task name in the **Name** field.

Step 4 Select the **Data Type** from the drop-down menu.

Step 5 Specify the **Files and Folders** Objects for the Backup Task.


Files and Folders
Empty Files and Folders
Empty Files and Folders
Default Folderset Files and Folder
Default CDP Files and Folders

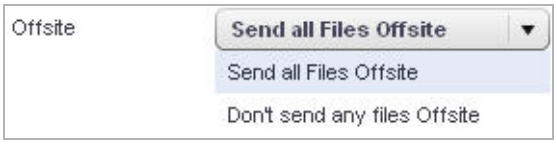
Step 6 Enter a numeric integer to specify the **Number of Versions** to retain for this backup.

Step 7 Choose a **trimming algorithm** to determine. Two options are available:

- **Delete Oldest**: Deletes backup files based on first item in, first item out method. **Delete Oldest** is only available for a **CDP** type backup.
- **Decay**: Deletes backup files based on a configured threshold. If the life of the backup file exceeds the configured threshold, then the backup file is deleted.

Step 8 Specify the desired **Offsite** option. Two options are available:

- **Send all files offsite**
- **Don't send any files offsite**



Step 9 Select the desired **Schedule** to apply to this Backup Task.

When a **Data Type** of **CDP** is selected, only **Interval** types of schedule objects will be listed in the **Schedule** drop-down menu.

When a **Data Type** of **FileSet** or **Application** is selected, only **Event** types of schedule objects will be listed in the **Schedule** drop-down menu.

Step 10 Click **OK** to create the new Backup Task.

About Trimming Algorithms

SonicWALL CDP offers two trimming algorithms:

- Delete Oldest
- Decay

If you are using the Decay option, it will work as described in the following example. As a hypothetical, assume you have backed up a file once per day for a year. After one year of Decay mode trimming, the final end result of revisions may look like this:

- 1 revision from a year ago
- 1 revision from 6 months ago
- 2 revisions from 3 months ago
- 3 revisions from this month

The Decay mode uses internal logic that attempts to give a broad range of revisions over time, with an emphasis on more recent revisions. This was the standard behavior used in SonicWALL CDP versions 3 through 5.0.

The Delete Oldest algorithm is linear (the same as application trimming in CDP 5.x). If you configure it to save 5 revisions and the 6th comes in, the oldest revision chronologically recorded will always be the one that is deleted.

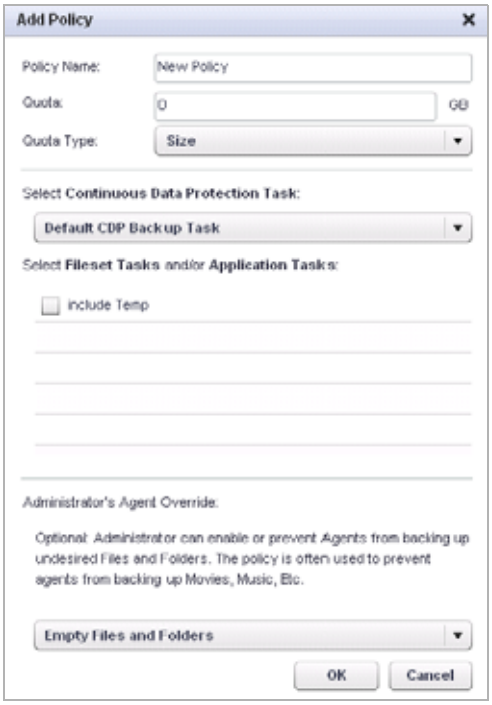
Creating a Global Policy

The Policy > Admin Policies page allows you to create global policies. A global policy is pushed out to all agents. Users can view or add to the global policy, but cannot delete it or remove anything from it. A global policy is created by combining a Backup Task object and a Files and Folders object.

To create a global policy, perform the following steps:

Step 1 Navigate to **Policy > Admin Policies**.

Step 2 Click the **+** button located in the bottom-right below the Policy > Admin Policies table. An **Add Policy** window appears.



Step 3 Enter a descriptive **Policy Name**.

Step 4 Enter a **Quota** in gigabytes. This is the amount of storage on disk available to agents that inherit this policy.

Step 5 Select either **Size** or **Size on Disk** for the **Quota Size**.

Size is calculated by adding up the sizes of each backed up file, as reported on the agent file system. **Size on Disk** is calculated from the actual storage space required on the SonicWALL CDP appliance, which can be considerably smaller than **Size**, because of data de-duplication. For information about data de-duplication, see the "About Data De-Duplication" section on page 10.

An agent that inherits this policy will be able to back up more data for a given Quota if **Size on Disk** is selected.

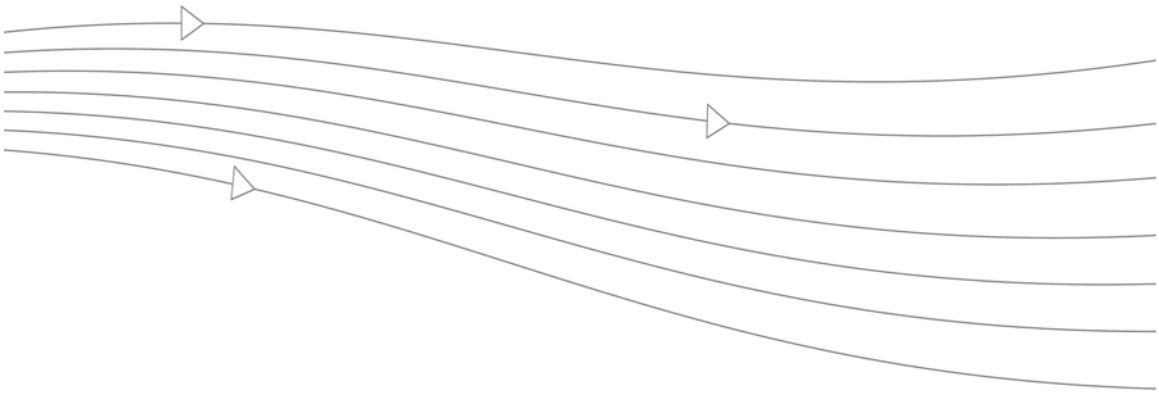
Step 6 Under **Select Continuous Data Protection Task**, select the CDP type backup task to be used in this policy. This task provides agents with a CDP type backup task to which they can add files and folders for continuous backup.

Step 7 Under **Select Fileset Tasks and/or Application Tasks**, select the checkboxes for any Fileset or Application type backup tasks that should be included in this global policy. These tasks define files or client applications that must be backed up on each agent that inherits this policy.

Step 8 Under **Administrator's Agent Override**, select a Files and Folders object that defines files or folders to be excluded and prevented from backup by the agent.

Step 9 Click **OK** to implement the new policy.

You can assign this policy as the default for certain agents on the Agents > Manage page.



Chapter 6: Managing Agents

The Agents pages allow you to manage SonicWALL agents that are associated with the SonicWALL CDP appliance. Agents are individual user computers or servers that can connect to an appliance to back up files and application data.

See the following sections:

- “Agents Interface” section on page 86
- “Managing Agents” section on page 87
- “Browsing Agents Files” section on page 92
- “Viewing Agent Policy Summaries” section on page 94
- “About the Agent User Interface” section on page 94
- “Using the Agent UI as Administrator” section on page 96

Agents Interface

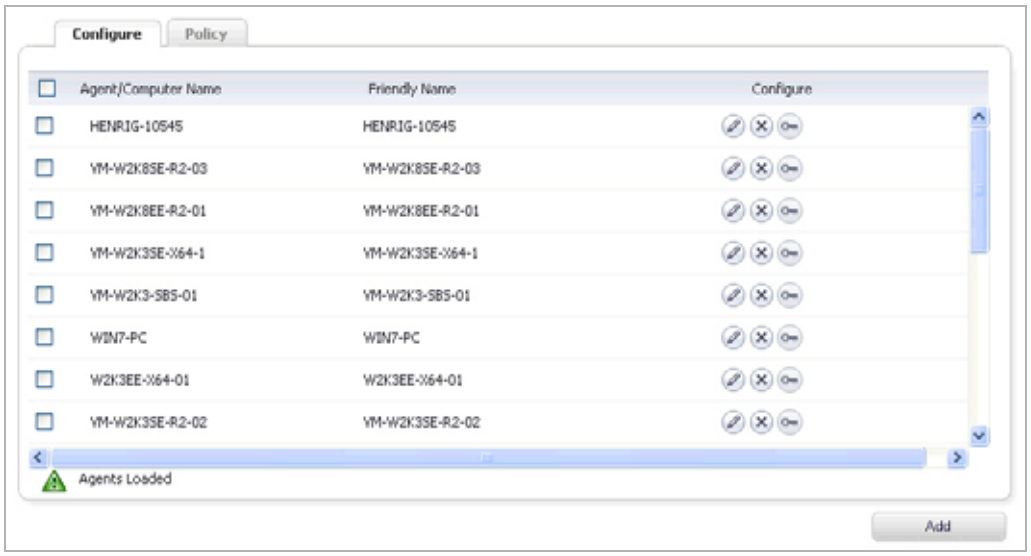
The Agents Interface options allow administrators to manage and browse agents, agent policies, and agent files.

The Agents function provides configuration options for agents assigned to the appliance, including a display of the agents currently backing up. The administrator can add agents, edit agents, and remove agent applications and agent folders that have been backed up.

Agents Options	Description
Manage	Provides access to add or remove agents, configure agent names, and select agent policies.
Browse Agent Files	Provides access to browse agent files. For each agent, you can view the backup tasks, file size, quota status, and other details. Backed up agent files can be removed from the SonicWALL CDP appliance.
Policy Summary	Provides a summary of each policy that is configured on the appliance.

Managing Agents

This section provides configuration information for the Agents > Manage page in the Web Management Interface.



This section includes the following subsections:

- "Adding a New Agent Friendly Name" section on page 88
- "Editing an Agent's Name" section on page 89
- "Resetting an Agent's Key" section on page 90
- "Deleting an Agent" section on page 90
- "Selecting an Agent's Policy" section on page 91

Adding a New Agent Friendly Name

The Add New Agent feature within the Web Management Interface allows the administrator to add friendly names for agents to SonicWALL CDP. SonicWALL CDP recognizes agents by agent name, which is the same as the computer name. Follow the tasks in this section to add a friendly name for an agent whenever you have a new server, laptop or PC that you would like to backup using SonicWALL CDP.

Adding an agent to a SonicWALL CDP appliance is accomplished by installing the Agent software on the agent computer, then launching it and connecting to the appliance. For instructions on installing the Agent software on a client computer, refer to the *SonicWALL CDP Agent User's Guide*.

To add a friendly name for an agent, perform the following steps:

Step 1 In the Web Management Interface, navigate to the **Agents > Manage** page.

Step 2 On the **Configure** tab, click the **Add** button to open the Configure dialog box.

Step 3 Enter the name of the agent you want to add in the **Agent Name** field.

The agent name is the same as the computer name. On Windows, the computer name can be viewed and edited by right-clicking **My Computer**, selecting **Properties**, and clicking the **Computer Name** tab.

Step 4 Type a descriptive name for the agent in the **Friendly Name** field.

Step 5 Click **OK** to add the friendly name for the agent.

To exit the dialog box without making any changes, click **Cancel**.

Step 6 Install the SonicWALL CDP Agent application on the added computer, if it is not already installed.

Editing an Agent's Name

The Edit Name function allows the administrator to change an inoperable agent's name in the Web Management Interface. SonicWALL CDP recognizes agents by agent name, which is the same as Computer Name.

In order to recover backed up data from an agent that has been rendered inoperable, it is necessary to change the name of that agent in Web Management Interface to match the name of a new agent. The new name must be the same as the computer name of the new agent.

Editing an inoperable agent's name to match a new agent allows Web Management Interface to recognize the new agent and associate backed up data from the inoperable agent with the newly assigned agent.

Note The Edit Name function should only be used to recover data from disabled agents. An alternate solution is to configure the new agent with the same computer name as the disabled agent. To change the computer name, right click **My Computer** and select **Properties**. Click the **Computer Name** tab and select **Change**, then type in the computer name of your previous computer.

To edit an agent's name in the Web Management Interface, perform the following steps:

Step 1 In the Web Management Interface, navigate to the **Agents > Manage** page.

Step 2 On the **Configure** tab, click the **Edit Agent** icon in the **Configure** column for the agent you want to rename. The edit dialog box opens.

Step 3 Type the new name for the agent computer in the **Agent Name** field.

Step 4 Type a descriptive name for the agent in the **Friendly Name** field.

Step 5 Click **OK**.

To exit the dialog box without making any changes, click **Cancel**.

Resetting an Agent's Key

The first time an agent computer communicates with a SonicWALL CDP appliance, it securely requests a security key, which will be stored in the local registry and used for future validation.

The administrator may need to reset the security key for an agent. To reset the security key, perform the following tasks:

Step 1 In the Web Management Interface, navigate to the **Agents > Manage** page.

Step 2 On the **Configure** tab, click the **Reset Security Key** icon in the **Configure** column for the agent whose key you want to reset.

Step 3 A status message displays near the bottom of the page to confirm the reset.

Deleting an Agent

The administrator can delete agents in the Web Management Interface. Deleting an agent allows the administrator to remove the rights of an agent to connect to the SonicWALL CDP appliance. If an agent is deleted and tries to connect, the agent will be blocked from connecting or backing up to the SonicWALL CDP.

Deleting an agent requires the following two steps:

- Deleting the agent using the Web Management Interface.
- Uninstalling the Agent software from the agent.

If a user uninstalls the Agent software from an agent, or removes the agent from the network, the agent settings will not be changed and previously backed up data will remain on the SonicWALL CDP appliance. Similarly, if an administrator deletes an agent, and the Agent software remains on the agent computer, the agent will reappear in the Web Management Interface at the next startup.

Note If you delete an agent from the agents list in the Web Management Interface, any data associated with the agent will be purged from the appliance.

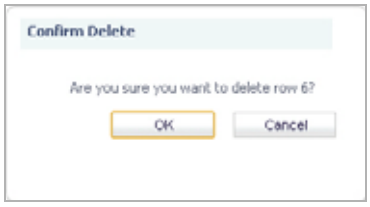
To delete an agent in the Web Management Interface, perform the following steps:

Step 1 In the Web Management Interface, navigate to the **Agents > Manage** page.

Step 2 On the **Configure** tab, click the **Delete Agent** icon in the **Configure** column for the agent you want to remove.

Step 3 Click **OK** in the confirmation dialog box.

To exit the dialog box without making any changes, click **Cancel**.



Step 4 Uninstall the Agent software from the agent computer, if you have not already done so.

Selecting an Agent's Policy

The administrator can assign an agent to a new administrative policy. If an agent is moved from a default policy to a custom policy, the data previously backed up will remain on the appliance. However, if the agent is moved from a custom policy to a different custom policy, the data previously backed up will be purged from the appliance.

To select an agent's policy, perform the following steps:

Step 1 In the Web Management Interface, navigate to the **Agents > Manage** page.

Step 2 Click the **Policy** tab

Step 3 Click the **Edit Policy** icon in the **Change Policy** column for the agent you want to edit. The edit dialog box opens.

Step 4 Select a policy from the **Select Admin Policy** drop-down list.

Step 5 Click **OK**.

To exit the dialog box without making any changes, click **Cancel**.

Browsing Agents Files

The Agents > Browse Agents Files page allows the administrator to view agent files and applications that are configured for backup, and to make changes to the SonicWALL CDP appliance, such as deleting backed up data.

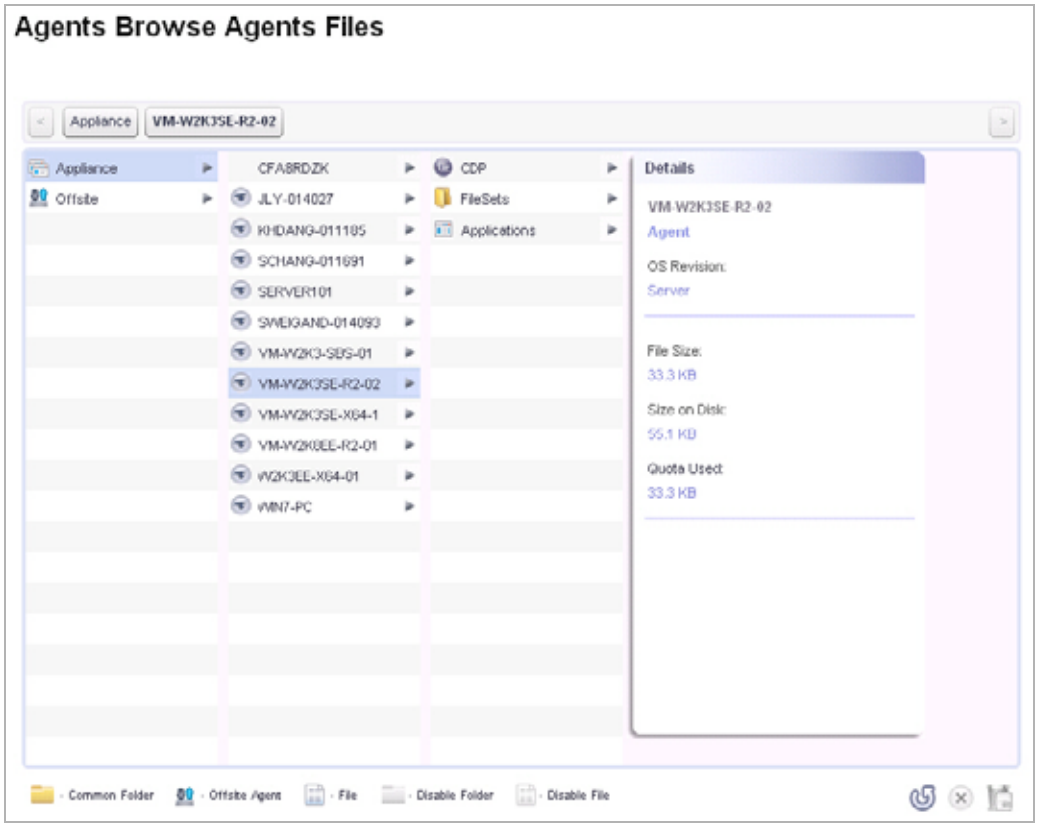
Note Deleting backed up data from the SonicWALL CDP appliance may need to be accompanied by changing the Backup Task in **Policies > Backup Tasks**. Otherwise, another revision of the same data will be backed up on the appliance at the next scheduled backup.

To browse and manage agent backups, perform the following steps:

Step 1 In the Web Management Interface, navigate to the **Agents > Browse Agents Files** page.

Step 2 Select the arrow for either **Appliance** or **Offsite** to expand the view to the agents that are configured to use either a local SonicWALL CDP appliance or an offsite appliance for backups.

Step 3 Click the arrow next to the agent you wish to browse.



Step 4 After you select the Agent, click one of the three types of backups: **CDP**, **FileSets**, or **Applications**.

Step 5 Continue clicking the arrows next to the items you wish to browse. To go back to a previous level, click the button for that level along the top of the browse section.

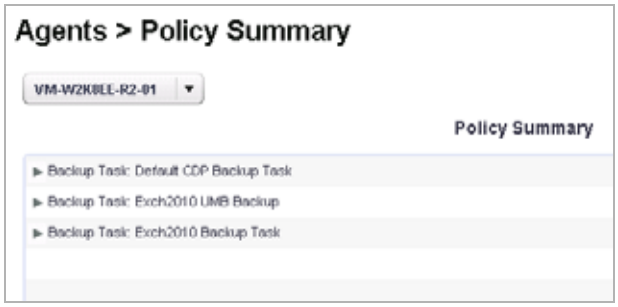
Step 6 To remove a backed up item from the appliance, select the item and then click the **Remove Item** icon at the bottom of the browse window.

Deleting backed up data from the SonicWALL CDP appliance may need to be accompanied by changing the Backup Task in Policies > Backup Tasks. Otherwise, another revision of the same data will be backed up on the appliance at the next scheduled interval.

Step 7 To remove a backed up item that no longer exists on the agent, select the item and then click the **Remove Deleted Items** icon at the bottom of the browse window.

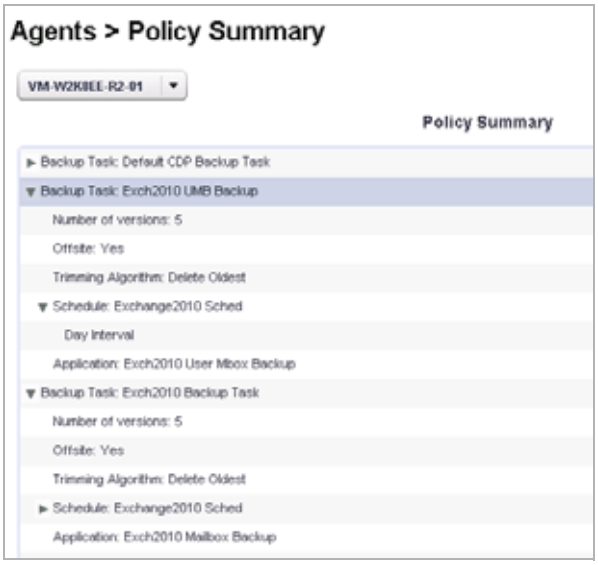
Viewing Agent Policy Summaries

The Agents > Policy Summary page allows you to view the policies that are configured for each agent.



Select the desired agent from the drop-down list, and the policy summary is refreshed with the associated list of policies.

To view more details about the displayed policies, click the arrow icons to expand the policies.



About the Agent User Interface

The SonicWALL CDP Agent User Interface provides individual users and system administrators the ability to configure, create, and apply local backup and restore policies on individual workstations. Users can set files and applications for backup (if so configured by the administrator in the Web Management Interface) and can recover backed up files.

The SonicWALL CDP Agent software is installed on every agent (server, laptop or PC intended to be backed up on the SonicWALL CDP Appliance). The SonicWALL Agent Service is installed automatically with the Agent User Interface and runs in the background, communicating with the SonicWALL CDP appliance. The administrator can elect to install just the Agent Service on agent machines, without installing the the Agent User Interface.

The Agent User Interface is the same on Windows, Linux, and Mac OS computers.

Agent User Interface Overview

The Agent User Interface includes four tabs or pages: **Status**, **My Backups**, **Policies**, and **Help**. User access to these pages is granted and administered by the administrator using the Web Management Interface. Table 1 provides an overview of the four default Agent User Interface controls:

Table 1 Agent User Interface Pages

Page	Description
Status	**Status** provides the user with the SonicWALL CDP appliance IP address, the agent name and state, quota information including file count, size, size on disk, quota remaining, and the current backup policy name. Recent tasks are displayed in right pane with task name, start time, duration, and status.
My Backups	**My Backups** provides access to all backed up data, including backups created using the CDP, FileSets, and Applications backup methods. It also provides the ability to enable or disable file or folder backups, refresh the display, search by all or part of the file name, restore data, remove items, and remove old file versions.
Policies	**Policies** provides the user with access to all backup status and configuration pages, including Summary, Files and Folders, Applications, Schedules, and Backup Tasks. Users can configure and schedule backups on the Policies tab.
Help	**Help** provides links to online help, the SonicWALL knowledge base, the Agent log file, and Agent version information.

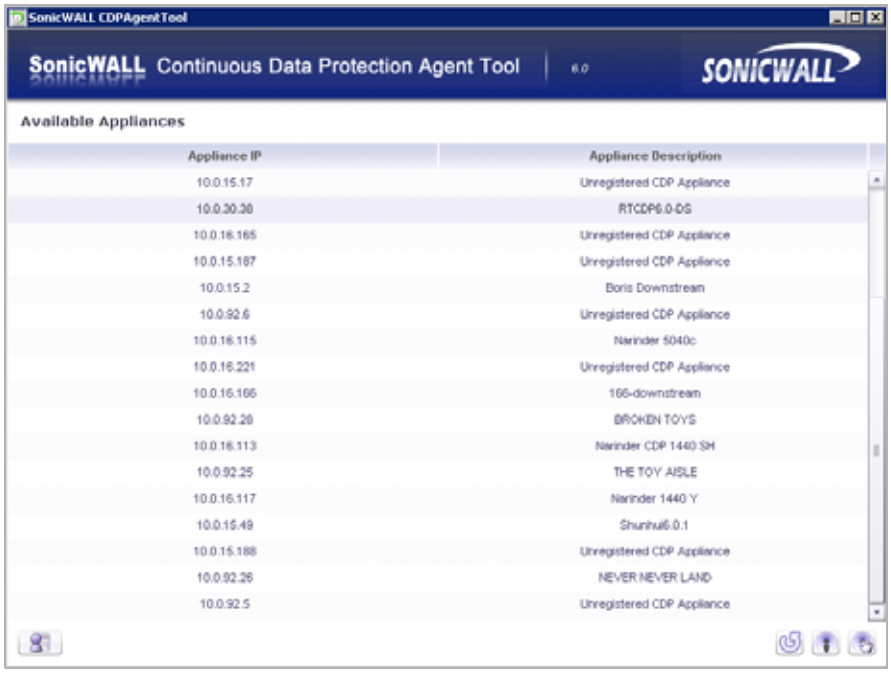
Note For more information on using the SonicWALL CDP Agent User Interface, refer to the *SonicWALL CDP Agent User's Guide*.

Using the Agent UI as Administrator

The Agent software allows Administrators to log into the Agent User Interface to manage and configure agent backups. You can access any appliance, and then view, manage, or restore any files backed up by any agent that is associated with that appliance, when logged in as an administrator in the Agent User Interface.

When you launch the Agent User Interface, there is a button in the lower left pane that allows you to log in as an Administrator.

When you click the Change Appliance icon, this button appears in the lower left corner to allow you to log in as an Administrator.

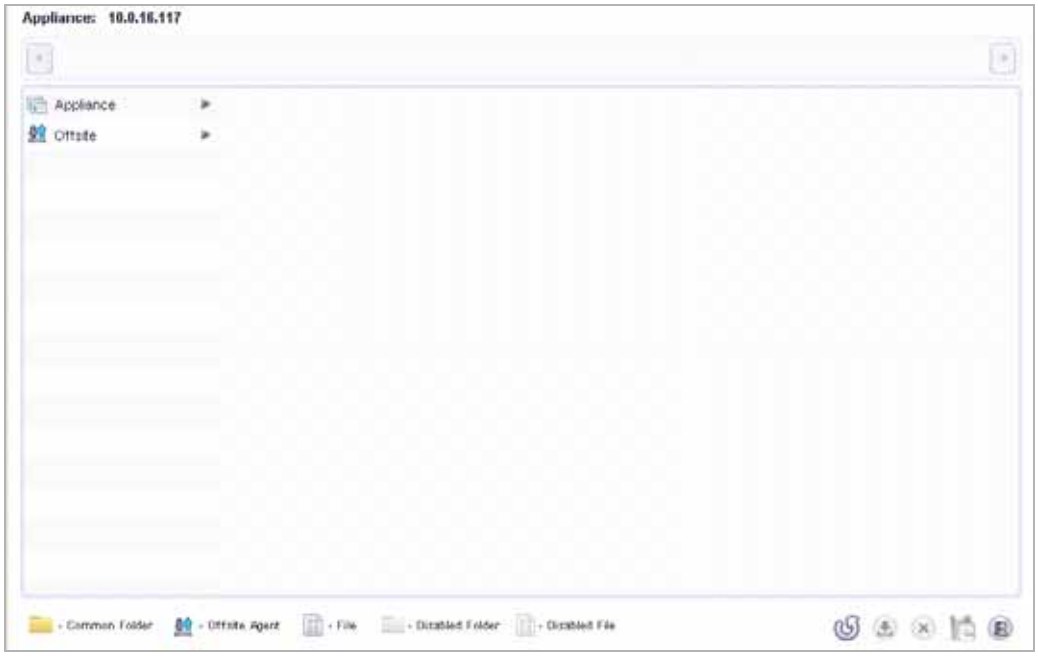


To log in and browse backed up files using the Administrator File Browser, perform the following steps:

Step 1 In the SonicWALL CDP Agent User Interface, click the **Login to Administrator File Browser** button.

Step 2 In the login dialog box, type in the IP address of the SonicWALL CDP appliance to which you want to connect.

Step 3 Type in the password for the admin account, and click **Login**. The Agent User Interface displays the starting screen for the appliance.



Step 4 Click the arrow for either **Appliance** or **Offsite** to expand the display to include all associated agents, then click any agent to expand the display further and view specific backups.

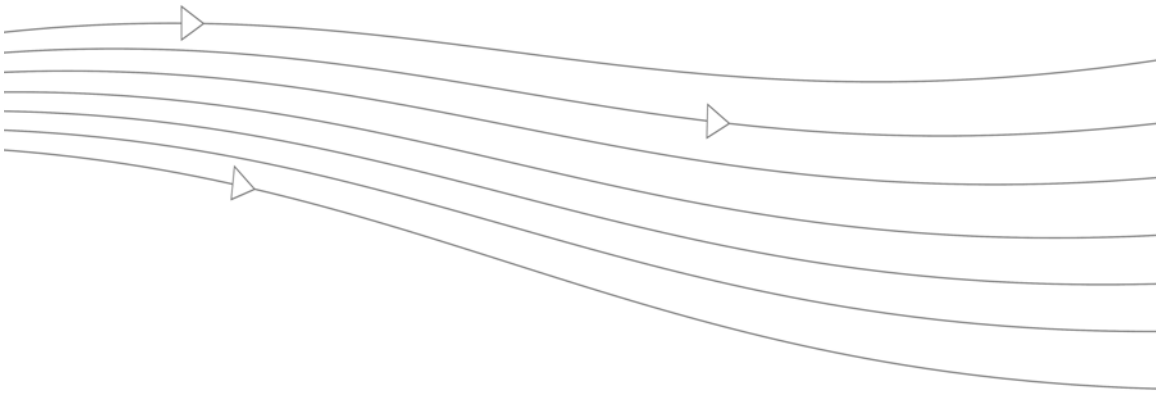
Step 5 The bottom of the window provides controls for your use.

Step 6 At the right, the following controls are available, from left to right:

- Refresh – refreshes the window contents
- Restore – restores the selected item
- Remove Items – removes the selected items
- Remove Deleted Items – removes items that are no longer on the agent machine
- Logoff from Administrator File Browser – logs off

Creating and Managing Backup Policies

While using the SonicWALL CDP Agent User Interface, an administrator creates and manages backup policies, schedules, and tasks the same way a user would using the Agent User Interface. Refer to the *SonicWALL CDP 6.0 Agent User Guide* for directions on creating and managing backup policies, schedules, and tasks.



Chapter 7: Bare Metal Recovery

This chapter provides information about the Bare Metal Recovery application, which can be used to create a whole-disk type of image on the SonicWALL CDP appliance. This chapter includes the following sections:

- "About Bare Metal Recovery" section on page 99
- "Configuring Bare Metal Recovery Accounts" section on page 100
- "Using Bare Metal Recovery" section on page 102

About Bare Metal Recovery

Bare Metal Recovery is a separate software product that can create a backup image of a whole disk or partition. A disk image backup includes a backup of operating systems, applications and configuration files, software updates, personal settings and other data.

One of the destinations for the image file can be an FTP server. The SonicWALL CDP appliance provides this capability by hosting SonicWALL Bare Metal Recovery **.tib** files.

Bare Metal Recovery Interface Overview

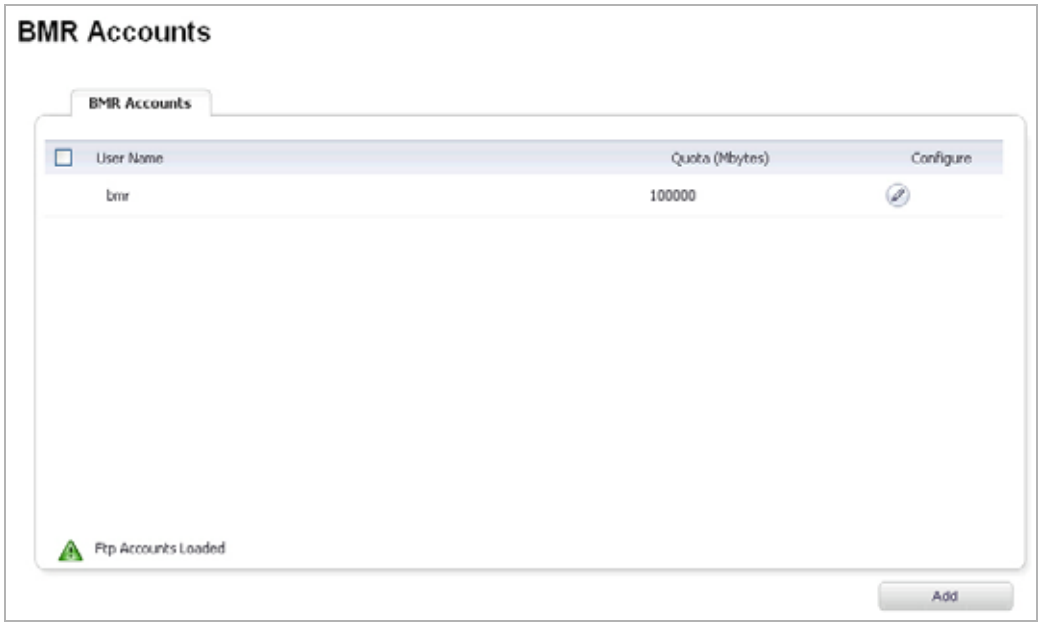
The Bare Metal Recovery (BMR) Interface allows the administrator to register BMR accounts.

BMR Options	Description
Accounts	Provides access to create and configure Bare Metal Recovery Accounts.

Configuring Bare Metal Recovery Accounts

SonicWALL System Recovery with Universal Restore (also known as Bare Metal Recovery (BMR)) integration is provided in SonicWALL CDP 6.0. By enabling the SonicWALL CDP appliance as an FTP server to allow read/write operations directly from the BMR tool, administrators no longer need a separate staging server and storage to write the BMR image before backing it up to the appliance.

The BMR > Accounts page provides the ability to add or edit an account for Bare Metal Recovery access.



See the following sections:

- “Adding a Bare Metal Recovery Account” on page 101
- “Editing a Bare Metal Recovery Account” on page 101

Adding a Bare Metal Recovery Account

To add an account that can be used to access the SonicWALL CDP appliance (as an FTP server) directly from the BMR tool, perform the following steps:

Step 1 In the Web Management Interface, navigate to the **BMR > Accounts** page.

Step 2 Click the **Add** button to open the BMR Accounts dialog box.

Step 3 Type the account username into the **username** field.

Step 4 Type the password for the account into the **password** field.

Step 5 Enter the number of megabytes that this account can use on the SonicWALL CDP appliance into the **quota** field.

Step 6 Click **Save**.

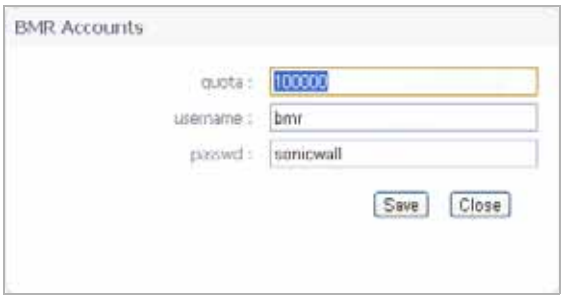
To exit the dialog box without saving, click **Close**.

Editing a Bare Metal Recovery Account

To edit an existing account, perform the following steps:

Step 1 In the Web Management Interface, navigate to the **BMR > Accounts** page.

Step 2 Click the **Edit Entry** icon in the **Configure** column for the account you want to edit. The BMR Accounts dialog box opens.



Step 3 Make the desired changes in the **quota**, **username**, or **password** fields.

Step 4 Click **Save**.

To exit the dialog box without saving, click **Close**.

Using Bare Metal Recovery

To use Bare Metal Recovery with the SonicWALL CDP appliance, you will need a user account on the appliance with the desired quota. Then you can launch the BMR application and save the image to the SonicWALL CDP appliance.

To use Bare Metal Recovery to save an image on the SonicWALL CDP appliance, perform the following steps:

Step 1 Create a user account on the SonicWALL CDP appliance, with the desired quota.

Step 2 Launch the BMR application and select the local drive or location that you want to back up.

Step 3 When the backup wizard prompts you for the destination at which to save the image, select **FTP Connections** and browse for the server, which can be the SonicWALL CDP appliance.

If the server is not listed, you can type in a path in the form:
ftp://<CDP IP Address>/upload/image.tib

where image.tib can be any file name with a **.tib** extension.

Step 4 When prompted for credentials, enter the credentials you created in step 1.

The BMR application performs the backup.

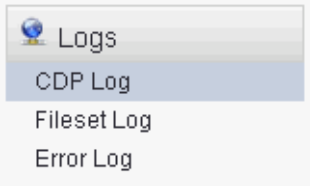
Chapter 8: Viewing the Logs

This chapter provides information about the SonicWALL CDP Log pages. See the following sections:

- “Logs Interface Overview” section on page 103
- “Viewing the CDP Log” section on page 104
- “Viewing the Fileset Log” section on page 105
- “Viewing the Error Log” section on page 106

Logs Interface Overview

The Logs pages provide administrators with navigation options to view appliance activity and event details.



Log Options	Description
CDP Log	Provides details about the CDP Process for backup/restore activity.
Fileset Log	Provides details about Fileset backup/restore activity.
Error Log	Provides details about CDP related errors and alerts.

Viewing the CDP Log

The Logs > CDP Log page displays log messages for activity resulting from the CDP process for backup and restore. When using the CDP process, files in a given folder are backed up as separate entities. Interval timer scheduling is used in the CDP process, so the scheduling is always on, and can have a configured start and end time for the backups to occur.

Figure 1 shows the Logs > CDP Log page.

Figure 1 Log for CDP Process

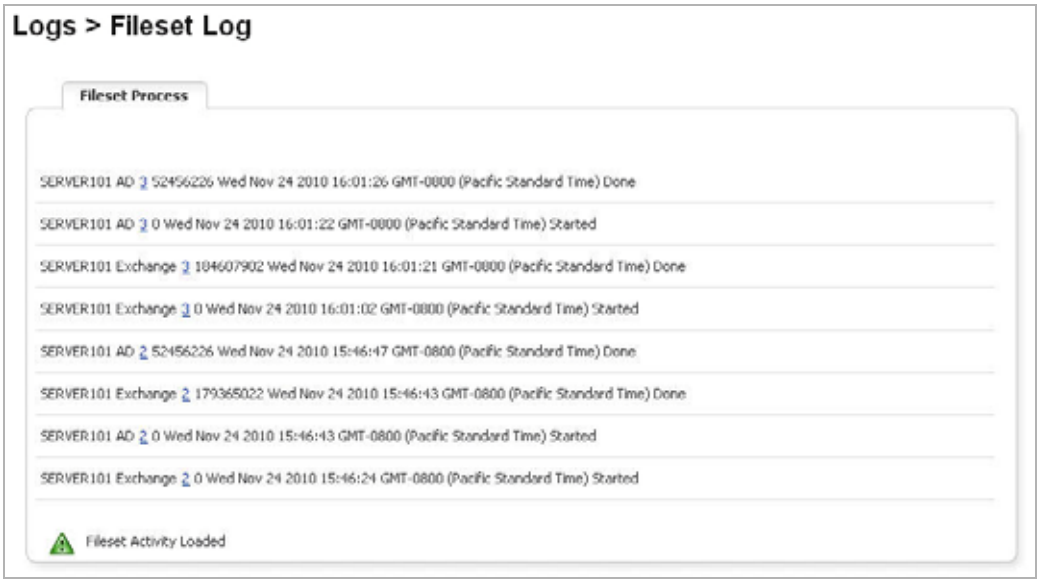
Logs > CDP Log
CDP Process
CFA8RDZK SERVER101/C:/50MB files/50-MB-File-1000001-01.txt 52377570 Wed Nov 24 2010 15:13:06 GMT-0800 (Pacific Standard Time)
CFA8RDZK SERVER101/C:/50MB files/abc/Directory Attributes 0 Wed Nov 24 2010 15:13:06 GMT-0800 (Pacific Standard Time)
CFA8RDZK SERVER101/C:/50MB files/a test file.txt 8 Wed Nov 24 2010 15:13:02 GMT-0800 (Pacific Standard Time)
CFA8RDZK SERVER101/C:/50MB files/Directory Attributes 0 Wed Nov 24 2010 15:13:02 GMT-0800 (Pacific Standard Time)
CDP Activity Loaded

Viewing the Fileset Log

The Logs > Fileset Log page displays log messages for activity resulting from the FileSet process for backup and restore. When using the FileSet process, the group of folders and files or application data in the FileSet are treated by SonicWALL CDP as a single data entity, rather than each file being backed up independently.

Figure 2 shows the Logs > Fileset Log page.

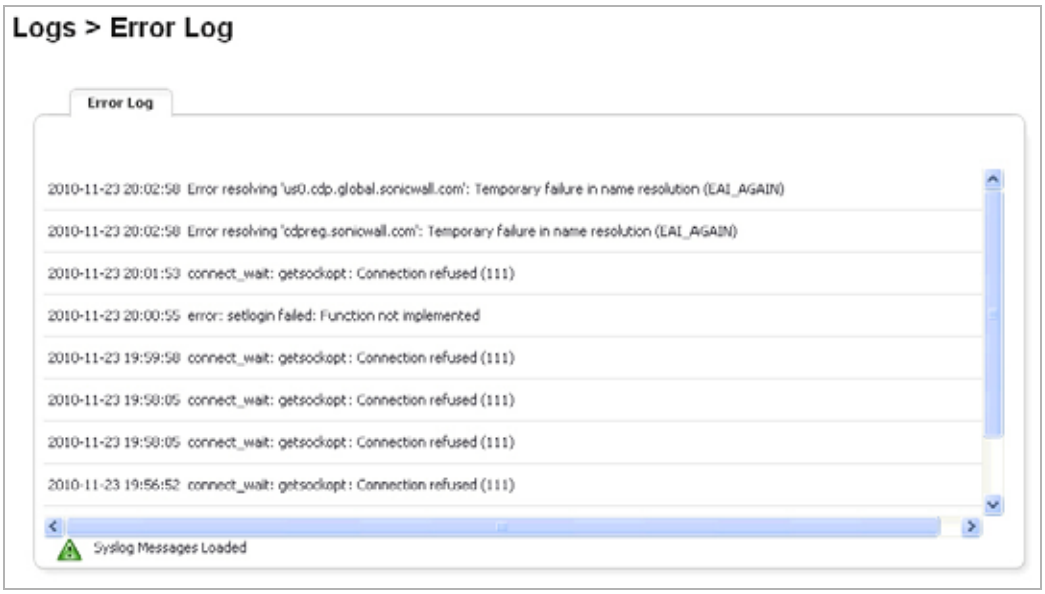
Figure 2 Log for Fileset Process

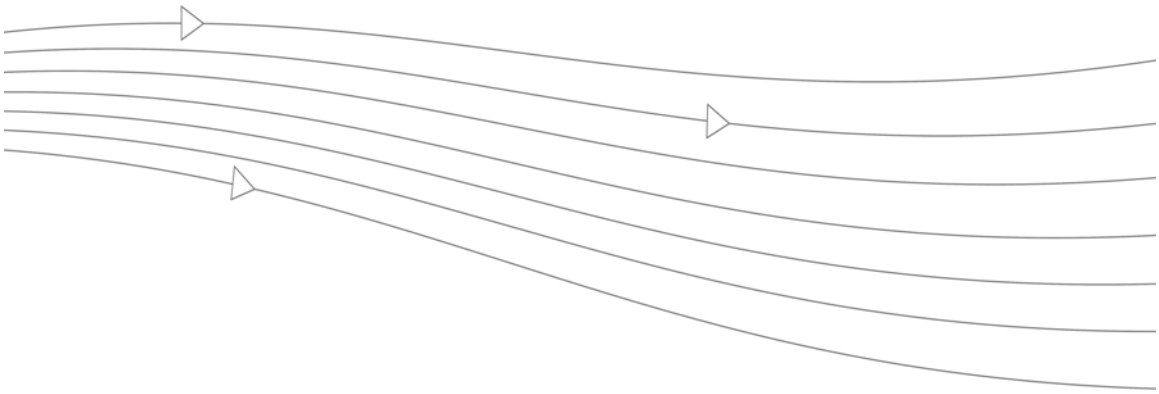

Logs > Fileset Log
Fileset Process
SERVER101 AD 3 52456226 Wed Nov 24 2010 16:01:26 GMT-0800 (Pacific Standard Time) Done
SERVER101 AD 3 0 Wed Nov 24 2010 16:01:22 GMT-0800 (Pacific Standard Time) Started
SERVER101 Exchange 3 184607902 Wed Nov 24 2010 16:01:21 GMT-0800 (Pacific Standard Time) Done
SERVER101 Exchange 3 0 Wed Nov 24 2010 16:01:02 GMT-0800 (Pacific Standard Time) Started
SERVER101 AD 2 52456226 Wed Nov 24 2010 15:46:47 GMT-0800 (Pacific Standard Time) Done
SERVER101 Exchange 2 179365022 Wed Nov 24 2010 15:46:43 GMT-0800 (Pacific Standard Time) Done
SERVER101 AD 2 0 Wed Nov 24 2010 15:46:43 GMT-0800 (Pacific Standard Time) Started
SERVER101 Exchange 2 0 Wed Nov 24 2010 15:46:24 GMT-0800 (Pacific Standard Time) Started
Fileset Activity Loaded

Viewing the Error Log

The Logs > Error Log page displays log messages for SonicWALL CDP errors and alerts. Figure 3 shows the Logs > Error Log page.

Figure 3 Logs > Error Log Page


Logs > Error Log
Error Log
2010-11-23 20:02:58 Error resolving 'us0.cdp.global.sonicwall.com': Temporary failure in name resolution (EAI_AGAIN)
2010-11-23 20:02:58 Error resolving 'cdpreg.sonicwall.com': Temporary failure in name resolution (EAI_AGAIN)
2010-11-23 20:01:53 connect_wait: getsockopt: Connection refused (111)
2010-11-23 20:00:55 error: setlogin failed: Function not implemented
2010-11-23 19:59:58 connect_wait: getsockopt: Connection refused (111)
2010-11-23 19:58:05 connect_wait: getsockopt: Connection refused (111)
2010-11-23 19:58:05 connect_wait: getsockopt: Connection refused (111)
2010-11-23 19:56:52 connect_wait: getsockopt: Connection refused (111)
Syslog Messages Loaded



Chapter 9: Configuring and Understanding Reports

The Reports pages provide the administrator with key reports on disk space usage and server status.

See the following sections:

- “Reports Interface Overview” section on page 108
- “Agent Summary Reports” section on page 109
- “Disk Space by File Type Reports” section on page 112
- “Disk Space Summary Reports” section on page 116
- “Detailed Event List Reports” section on page 117
- “Agent Events Summary Reports” section on page 119
- “Daily Events Summary Reports” section on page 120
- “Schedule Backup Reports” section on page 121
- “Configuring Scheduled Reports Delivered by Email” section on page 122

Reports Interface Overview

The Reports Interface allows administrators to navigate various reports listed in the Report Options. The reports provide administrators with details about disk usage and space, individual agents, event summaries, and schedule backups. Administrators can configure reports delivered by email.

Options	Description
Agent Summary	Displays a summary about Agent details. Refer to “Agent Summary Reports” section on page 109 for more details.
Disk Space by File Type	Displays details about CDP and Fileset file types on the CDP appliance. Refer to “Disk Space by File Type Reports” section on page 112 for more details.
Disk Space Summary	Displays details about Agent quotas and total disk spaced used on the CDP appliance. Refer to “Disk Space Summary Reports” section on page 116 for more details.
Detailed Event List	Displays details about individual Agents. Refer to “Detailed Event List Reports” section on page 117 for more details.
Agent Events Summary	Displays details about Agent events. Refer to “Agent Events Summary Reports” section on page 119 for more details.
Daily Events Summary	Displays a summary of daily backup events. Refer to “Daily Events Summary Reports” section on page 120 for more details.
Schedule Backup	Displays details about schedule backups. Refer to “Schedule Backup Reports” section on page 121 for more details.
Configuration	Allows the administrator to configure reports. Refer to “Configuring Scheduled Reports Delivered by Email” section on page 122 for more details.

Agent Summary Reports

The Agent Summary Reports displays a bar graph and data table containing details about Agent quotas, disk usage, and file counts based on individual Agents.

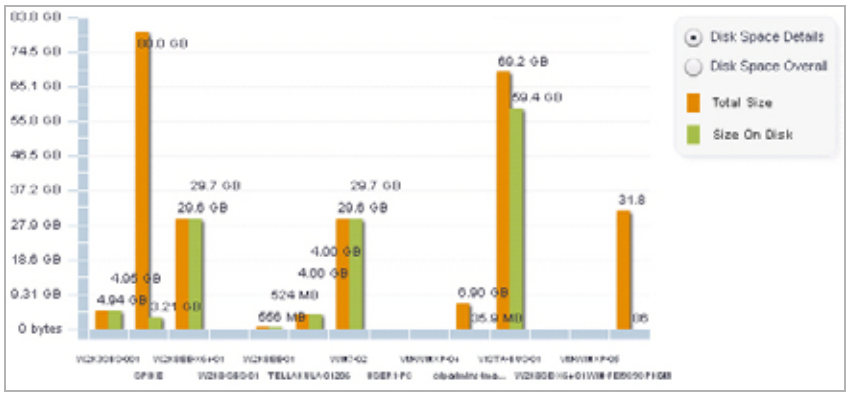
Figure 1 shows the Reports > Agent Summary page.

Figure 1 Agent Summary Report

Reports Agent Summary
Disk Space Details
Disk Space Overall
Total Size
Size On Disk
Agent Name | Quota | Size | Size On Disk | File Count | Policy Name
W2K3SBS-001 | 80.0 GB | 4.94 GB | 4.95 GB | 1 | Default Policy
SPIKE | 80.0 GB | 80.0 GB | 3.21 GB | 14 | Default Policy
W2K8EE-X64-01 | 80.0 GB | 29.6 GB | 29.7 GB | 003 | Default Policy
W2K8-SBS-01 | 80.0 GB | 0 bytes | 0 bytes | 0 | Default Policy
W2K8EE-01 | 80.0 GB | 556 MB | 524 MB | 24 | Default Policy
TELLAKULA-01206 | 80.0 GB | 4.00 GB | 4.00 GB | 2 | Default Policy
WIN7-02 | 80.0 GB | 29.6 GB | 29.7 GB | 5 | Default Policy
USER1-PC | 80.0 GB | 0 bytes | 0 bytes | 0 | Default Policy

Agent Summary Graph

The Agent Summary graph allows administrators to compare disk usage among Agents. The legend located to the right of the graph defines the colors seen in the graph. Located above the legend are viewing options. The **Disk Space Details** and **Disk Space Overall** are two viewing options available to display the Agent Summary details.

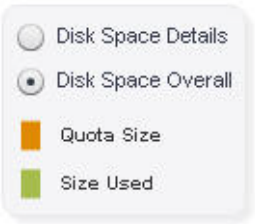


Changing Graph Views

Changing the graph views allows for viewing of individual agents' disk space usage and overall disk space usage.

To change the graph views:

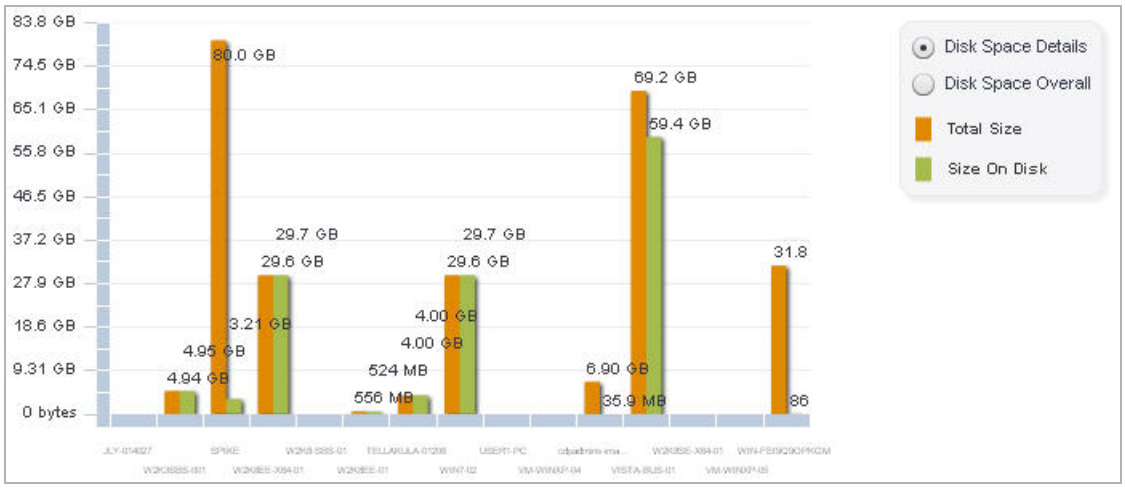
Step 1 Locate the two radio buttons above the legend and to the right of the pie chart.



Step 2 Select a viewing option. Two options are available: **Disk Space Details** or **Disk Space Overall**. The graph updates automatically when a radio button is selected.

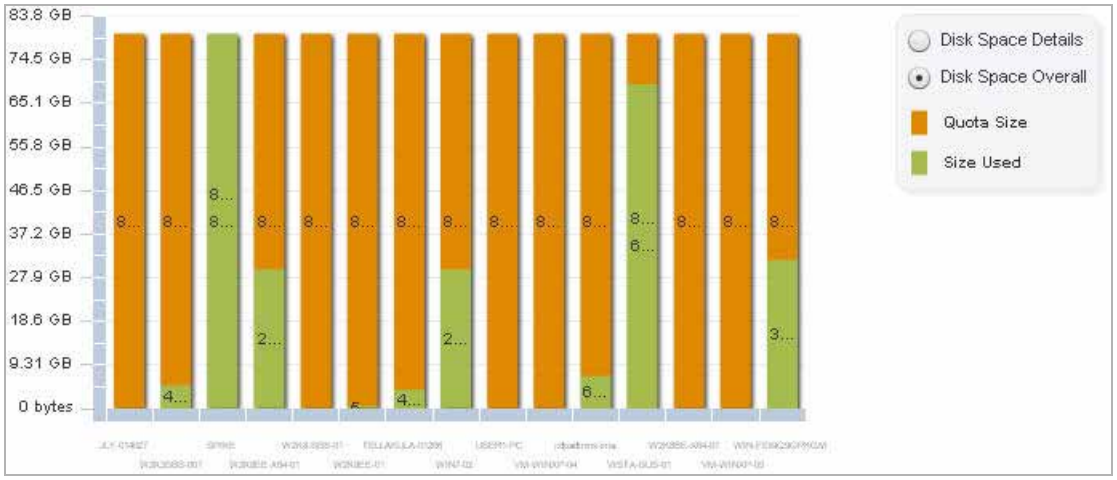
Disk Space Details

The Disk Space Details displays details about Disk Space usage and availability, based on individual Agents. The graph contains a x-axis indicating the Agent Name, y-axis indicating the amount of disk space in gigabytes (GB), a legend defining the colors seen in the graph, and viewing options located above the legend.



Disk Space Overall

The Disk Space Overall graph displays details about overall disk space on the appliance. The graph provides the administrator a visual representation of used and free disk space. The orange color represents the allotted quota size whereas the green color represents the amount of disk space used.



Agent Summary Table

The Agent Summary Table provides a detailed summary about individual agent disk usage.

Agent Name	Quota	Size	Size On Disk	File Count	Policy Name
W2K3SBS-001	80.0 GB	4.94 GB	4.95 GB	1	Default Policy
SPIKE	80.0 GB	80.0 GB	3.21 GB	14	Default Policy
W2K8EE-X64-01	80.0 GB	29.6 GB	29.7 GB	883	Default Policy
W2K8-SBS-01	80.0 GB	0 bytes	0 bytes	0	Default Policy
W2K8EE-01	80.0 GB	556 MB	524 MB	24	Default Policy
TELLAKULA-01206	80.0 GB	4.00 GB	4.00 GB	2	Default Policy
WIN7-02	80.0 GB	29.6 GB	29.7 GB	5	Default Policy
USER1-PC	80.0 GB	0 bytes	0 bytes	0	Default Policy

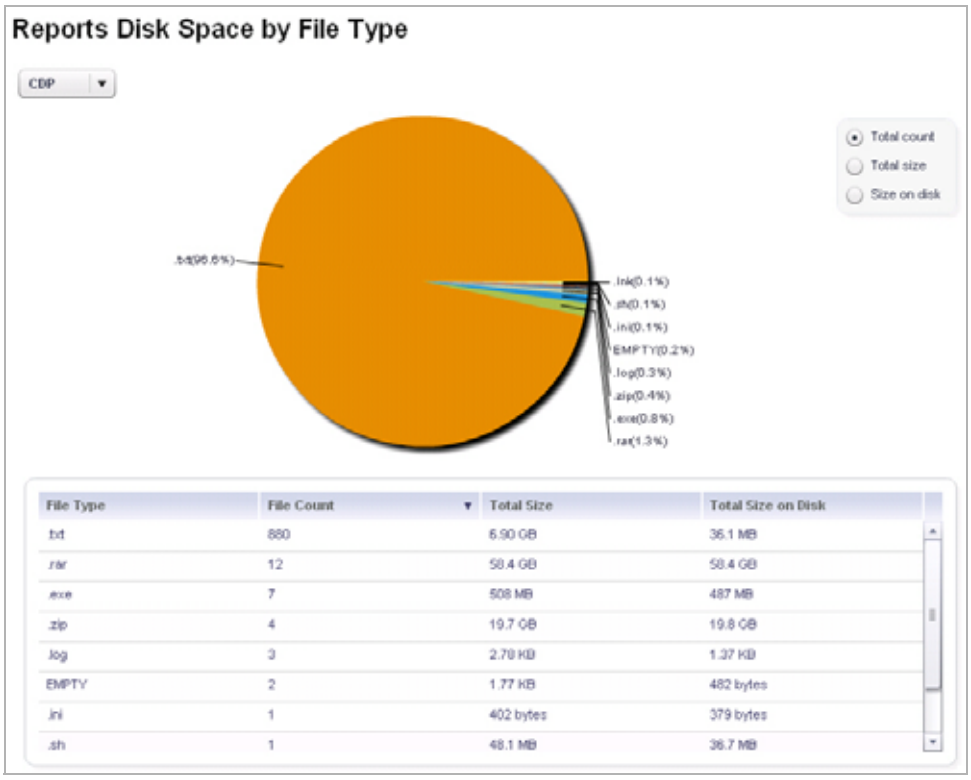
Column	Description
Agent Name	Displays the name of the agent.
Quota	Displays the Quota size allotted for the agent
Size	Displays the total size of all files.
Size on Disk	Displays the total size of all the files on the disk.
File Count	Displays the number of files backed up
Policy Name	Displays the name of the policy applied to the Agent.

Disk Space by File Type Reports

The Disk Space by File Type Reports displays details about the total amount of disk space used categorized by different file types. The report is comprised of a pie chart, viewing options, and data table. Each file type is labeled and represented by a color in the pie chart.

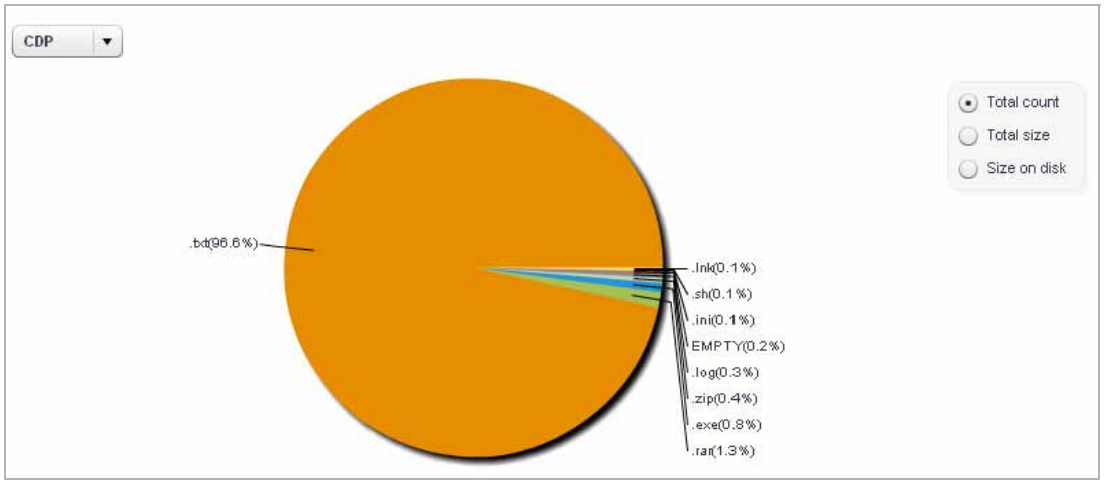
Figure 2 shows the Reports > Disk Space by File Type page.

Figure 2 Disk Space by File Type Report



Disk Space by File Type Chart

Changing the chart views allows for viewing of the total count, size, and size on disk of disk space organized by file type. The Total Count, Total Size, and Size on Disk are the three available viewing options.



Changing Graph Views

Alternate viewing options are available to help the administrator visualize the collected information.

To change the graph views:

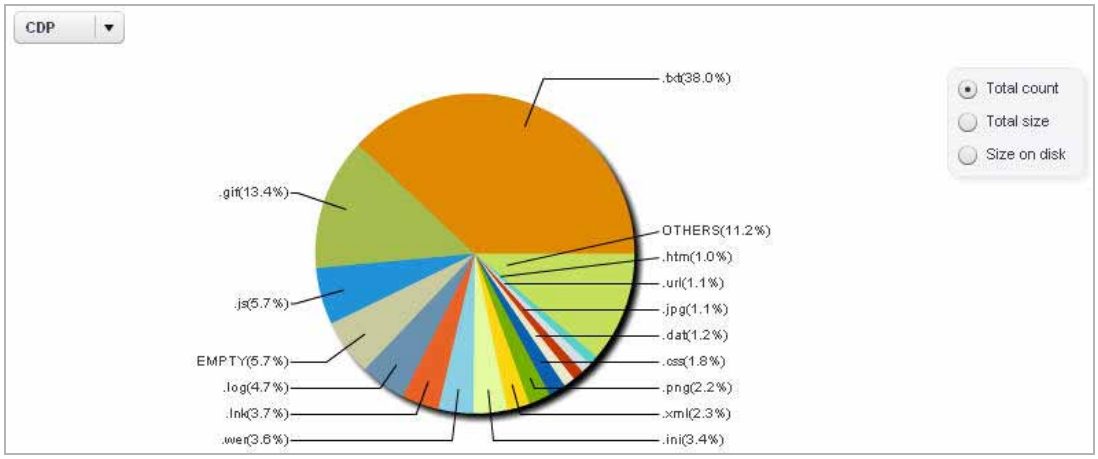
Step 1 Determine the desired view: the **CDP** disk space or **Fileset** disk space by file type. Select one of the two options available in the drop-down menu located to the upper-left of the pie chart.

Step 2 Locate the three radio buttons to the right of the pie chart and make a selection. Three options are available: **Total Count**, **Total Size**, and **Size on Disk**.

The data table changes accordingly to the graph view you select.

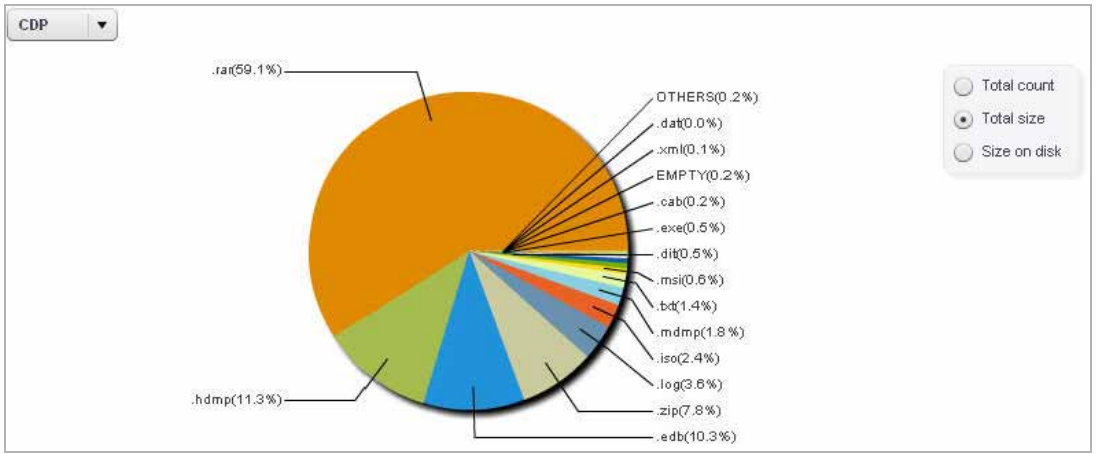
Total Count View

The Total Count View provides a visual representation of the total files allocated to the disk space of the appliance.



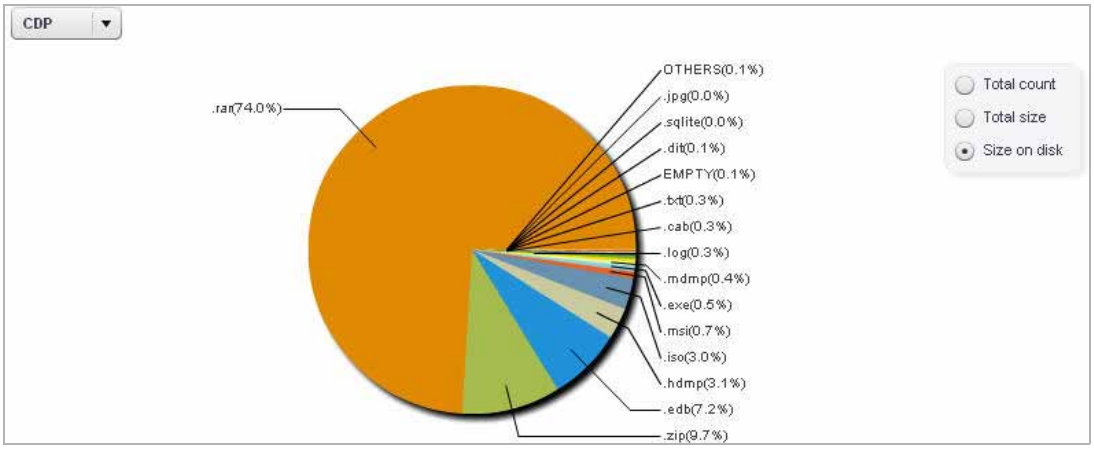
Total Size View

The Total Size View provides a visual representation of the size of all the files being backed up.



Size on Disk View

The Size on Disk View provides a visual representation of the total of all files on the disk.



Disk Space by File Type Table

The Disk Space by File Type Table provides a detailed summary about the various file types stored on the CDP appliance.

File Type	File Count	Total Size	Total Size on Disk
.txt	1412	354 MB	51.9 MB
.gif	497	399 KB	511 KB
.js	213	4.28 MB	1.41 MB
EMPTY	212	47.0 MB	27.4 MB
.log	173	937 MB	61.7 MB
.lnk	139	159 KB	90.3 KB
.wer	132	326 KB	112 KB
.ini	127	36.9 KB	48.0 KB

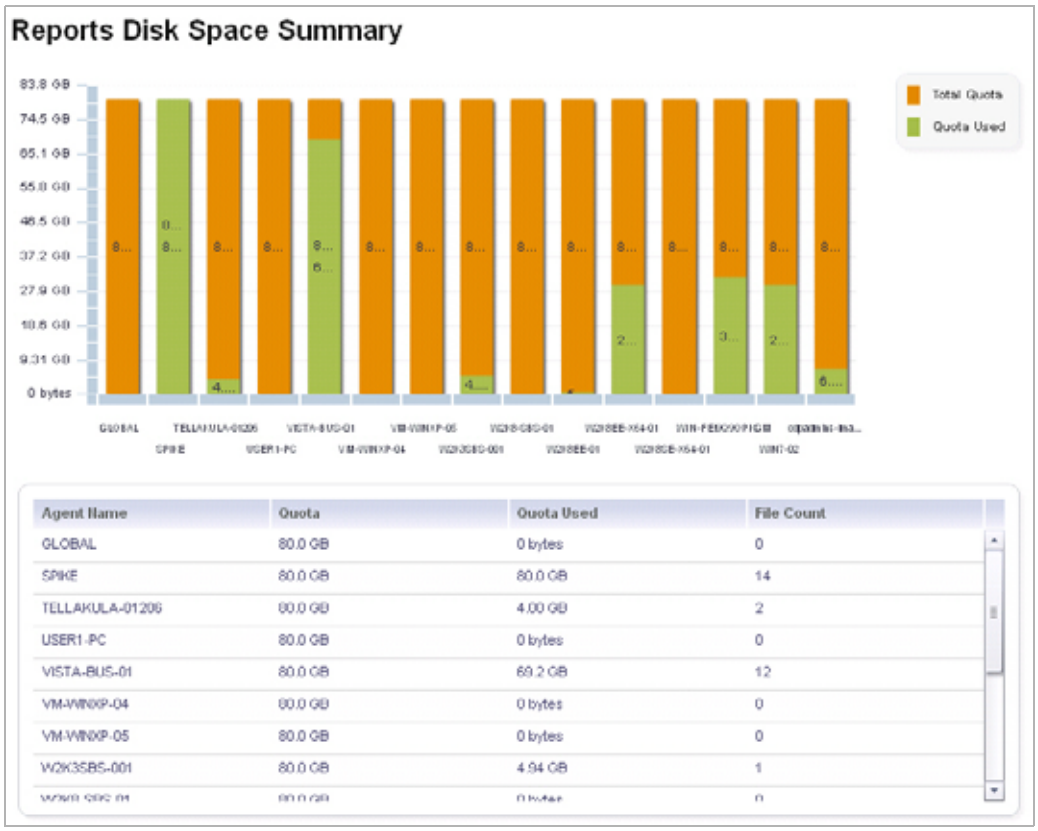
Column	Description
File Type	Displays the number of file types located on the appliance disk space.
File Count	Displays the number of files on the appliance disk space.
Total Size	Displays the total of all file sizes.
Total Size on Disk	Displays the total of all file sizes located on the appliance disk space.

Disk Space Summary Reports

The Disk Space Summary Reports display details about the amount of total disk space used by individual Agents.

Figure 3 shows the Reports > Disk Space Summary page.

Figure 3 Disk Space Summary Report



Graph

Changing the chart views allows for viewing of the total count, size, and size on disk of disk space organized by file type.

Table

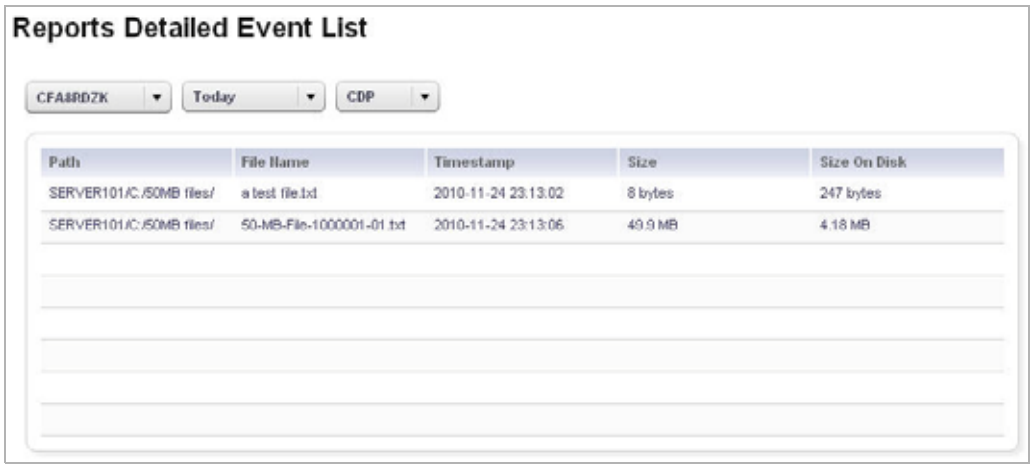
The Disk Space by File Type Table provides a detailed summary about the various file types stored on the CDP appliance.

Detailed Event List Reports

The Detailed Event List Report displays details about individual backup events including the filepath, file name, timestamp, size, and size on disk.

Figure 4 shows the Reports > Detailed Event List page.

Figure 4 Detailed Event List Report



Table

The Disk Space by File Type Table provides a detailed summary about the various file types stored on the CDP appliance.b

Detailed Event Display Options

Changing the graph views allows for viewing of individual agents' disk space usage and overall disk space usage.

To change the graph views:

Step 1 Locate the two radio buttons above the legend and to the right of the pie chart.

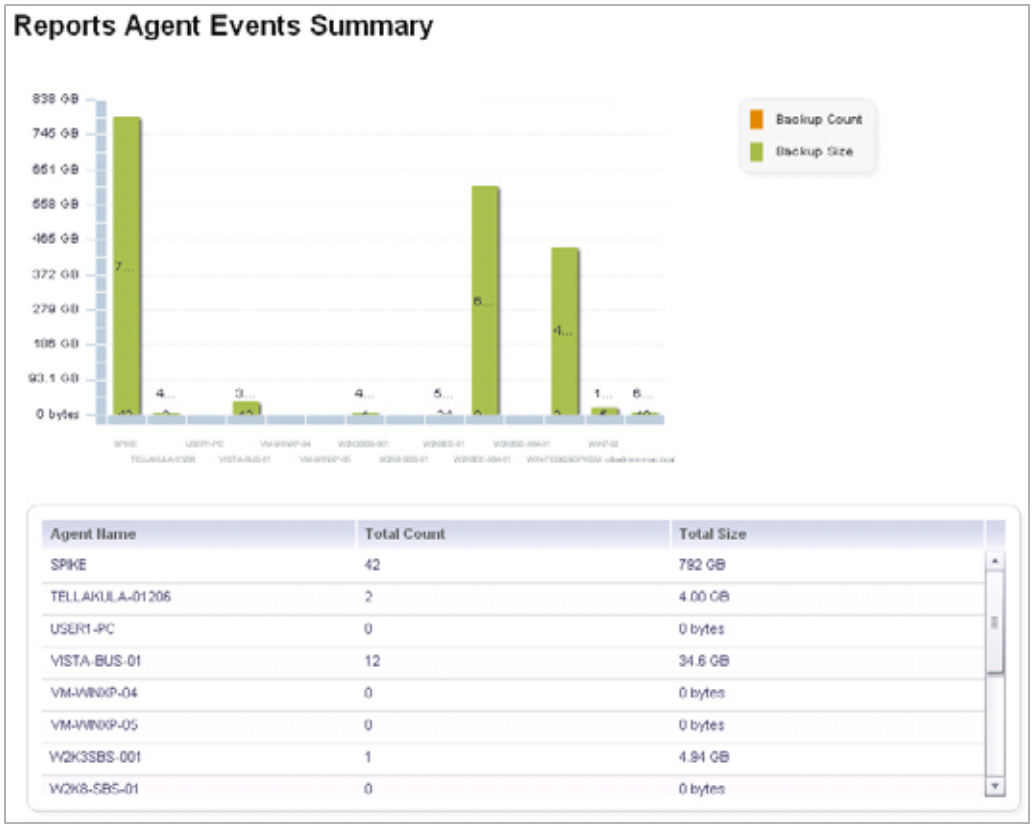
Step 2 Select a viewing option. Two options are available: **Disk Space Details** or **Disk Space Overall**. The graph view changes automatically when a radio button is selected.

Agent Events Summary Reports

The Agent Events Summary Report displays details about backup file count and backup file size information pertaining to individual agents.

Figure 5 shows the Reports > Agent Events Summary page.

Figure 5 Agent Events Summary Report



Agent Name	Total Count	Total Size
SPIKE	42	792 GB
TELLAKULA-01206	2	4.00 GB
USER1-PC	0	0 bytes
VISTA-BUS-01	12	34.6 GB
VM-WINXP-04	0	0 bytes
VM-WINXP-05	0	0 bytes
W2K3SBS-001	1	4.94 GB
W2K8-SBS-01	0	0 bytes

Graph

Changing the chart views allows for viewing of the total count, size, and size on disk of disk space organized by file type.

Table

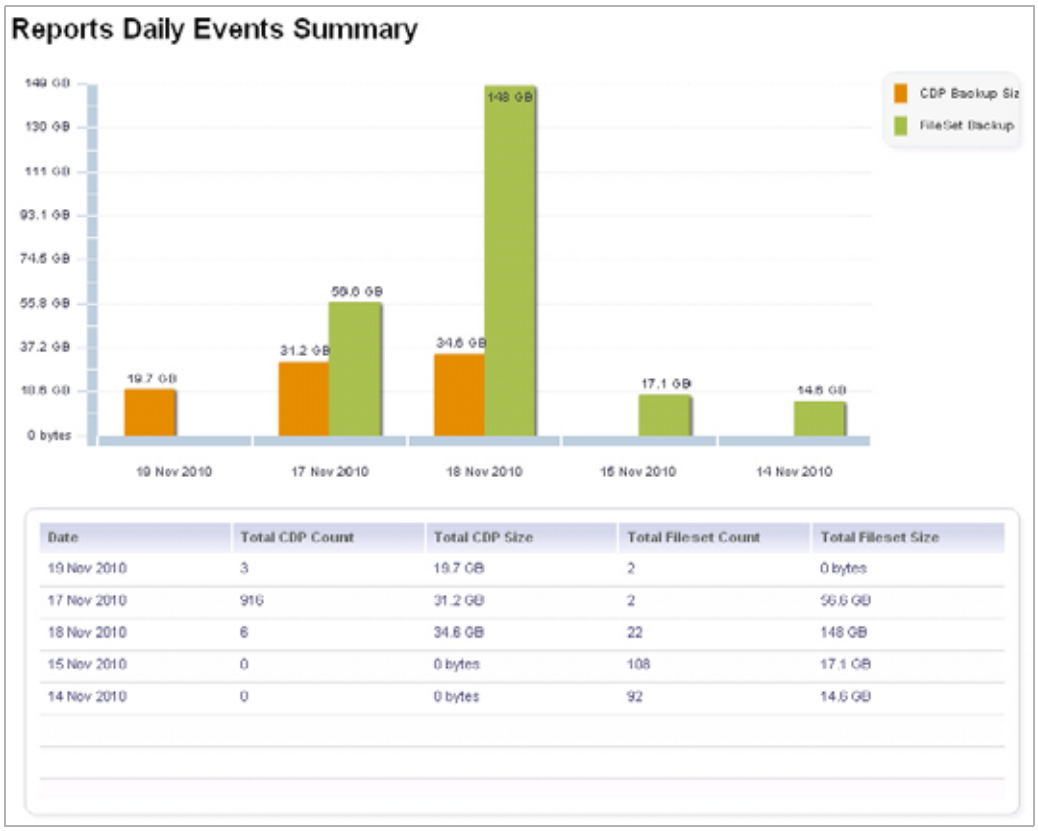
The Disk Space by File Type Table provides a detailed summary about the various file types stored on the CDP appliance.

Daily Events Summary Reports

The Daily Events Summary Reports displays details a daily summary of events that occurred on a specific date.

Figure 6 shows the Reports > Daily Events Summary page.

Figure 6 Daily Events Summary Report



Date	Total CDP Count	Total CDP Size	Total Fileset Count	Total Fileset Size
19 Nov 2010	3	19.7 GB	2	0 bytes
17 Nov 2010	916	31.2 GB	2	56.6 GB
18 Nov 2010	6	34.6 GB	22	148 GB
15 Nov 2010	0	0 bytes	108	17.1 GB
14 Nov 2010	0	0 bytes	92	14.6 GB

Graph

Changing the chart views allows for viewing of the total count, size, and size on disk of disk space organized by file type.

Table

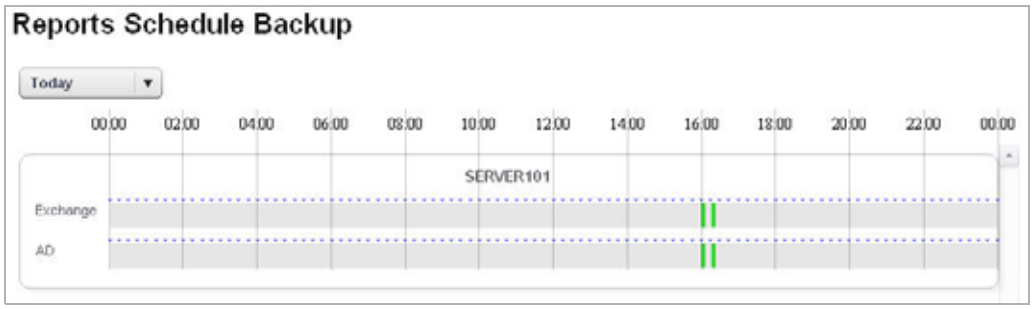
The Disk Space by File Type Table provides a detailed summary about the various file types stored on the CDP appliance.

Schedule Backup Reports

The Schedule Backup Reports displays a visual summary about scheduled backups that occurred today and within the past 2 days, 7 days, 14 days, and 30 days.

Figure 7 shows the Reports > Schedule Backup page.

Figure 7 Schedule Backup Selections



Graph

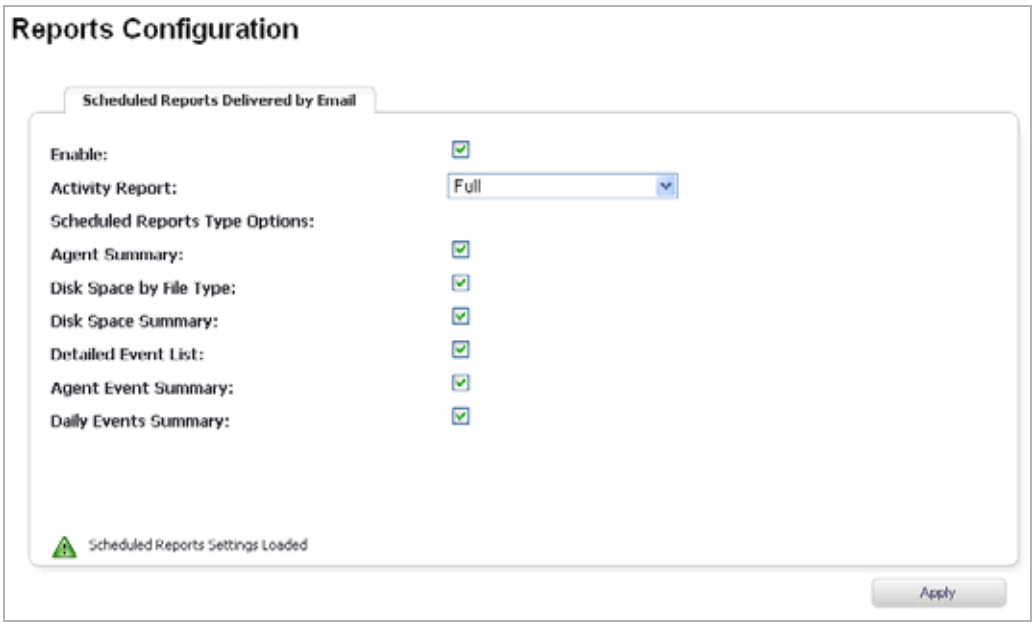
Changing the chart views allows for viewing of the total count, size, and size on disk of disk space organized by file type.

Configuring Scheduled Reports Delivered by Email

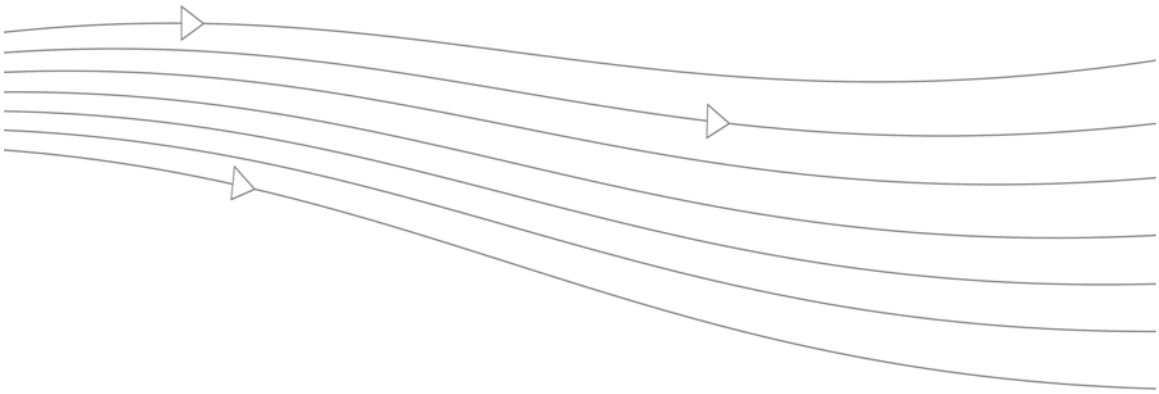
Administrators can configure SonicWALL CDP to deliver scheduled reports by email.

Figure 8 shows the Reports > Configuration page.

Figure 8 Reports Configuration Page



Options	Description
Enable	Enables the delivery of scheduled reports to the administrators email.
Activity Report	Allows the administrator to determine the amount of information displayed in the activity report.



Chapter 10: Backing Up Applications

This chapter provides information about backing up applications on the SonicWALL CDP appliance. This chapter includes the following sections:

- “Creating Schedules for Application Backups” section on page 124
- “Backing up Exchange 2010” section on page 126
- “Backing up Exchange 2007/2003” section on page 139
- “Backing Up SharePoint” section on page 151
- “Backing up System State and Active Directory” section on page 156
- “Backing up Microsoft SQL Server” section on page 161

Creating Schedules for Application Backups

To back up an application, you must configure an application object, a schedule, and a backup task that includes both the application object and the schedule. This section describes how to create the schedule object.

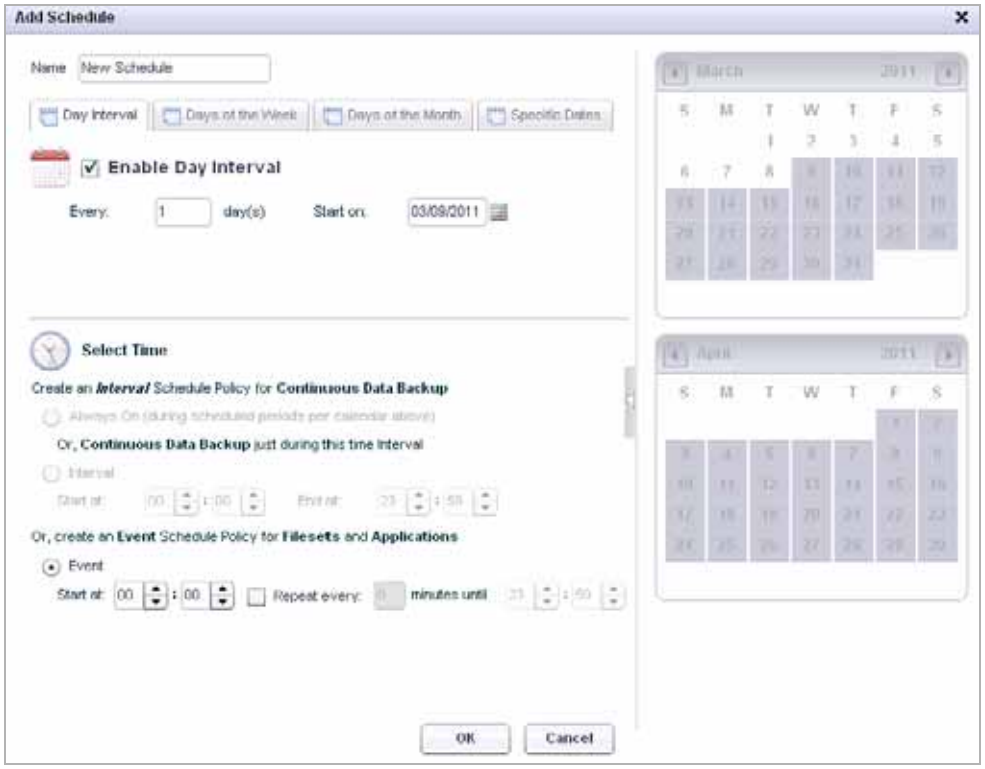
Note You can use the same schedule object in more than one backup task.

To configure a schedule for application backups, perform the following steps:

Step 1 In the SonicWALL CDP Agent User Interface, click the **Policies** tab.

Step 2 In the left pane, select **Schedules**.

Step 3 In the right pane, click the Plus button at the lower right corner. The Add Schedule window opens.


Add Schedule
Name New Schedule
Day Interval
Days of the Week
Days of the Month
Specific Dates
Enable Day Interval
Every: 1 day(s)
Start on: 03/09/2011
Select Time
Create an Interval Schedule Policy for Continuous Data Backup
Always On (during scheduled periods per calendar above)
Or, Continuous Data Backup just during this time interval
Interval
Start at: 00 : 00
End at: 23 : 59
Or, create an Event Schedule Policy for Filesets and Applications
Event
Start at: 00 : 00
Repeat every: 5 minutes until 23 : 59
OK
Cancel

Step 4 Type a descriptive name for the schedule into the **Name** field.

Step 5 Select one or more of the following tabs to configure a schedule that meets your requirements:

- **Day Interval** – The backup occurs every so many days calculated from a particular date.
  - Select the **Enable Day Interval** checkbox.
  - Select the number of days for the interval between backups.
  - Select a start date. By default, the interval is calculated from the current date.
  - Select the **Event** radio button.
  - Fill in the **Start at** fields by selecting an hour and a minute for the start time on the selected days.

  - To repeat the backup at intervals during the selected days, select the **Repeat** checkbox and type a value into the **Repeat every** ... **minutes** field, then select an hour and minute for the end time after **until**.

- **Days of the Week** – The backup runs on certain days of the week.
  - Select the **Enable Days of the Week** checkbox.
  - Select the days of the week, Sunday through Saturday, on which to run the backup.
  - Select the **Event** radio button.
  - Fill in the **Start at** fields by selecting an hour and a minute for the start time on the selected days.
  - To repeat the backup at intervals during the selected days, select the **Repeat** checkbox and type a value into the **Repeat every** ... **minutes** field, then select an hour and minute for the end time after **until**.
- **Days of the Month** – The backup occurs on certain days of the month.
  - Select the **Enable Days of the Month** checkbox.
  - Select the days of the month on which to run the backup. Select **Last** for the last day of the month.
  - Select the **Event** radio button.
  - Fill in the **Start at** fields by selecting an hour and a minute for the start time on the selected days.
  - To repeat the backup at intervals during the selected days, select the **Repeat** checkbox and type a value into the **Repeat every** ... **minutes** field, then select an hour and minute for the end time after **until**.
- **Specific Dates** – The backup occurs on the selected dates.
  - Select the **Enable Specific Dates** checkbox.
  - Click the small calendar and then select the date(s).
  - Select the **Event** radio button.
  - Fill in the **Start at** fields by selecting an hour and a minute for the start time on the selected days.
  - To repeat the backup at intervals during the selected days, select the **Repeat** checkbox and type a value into the **Repeat every** ... **minutes** field, then select an hour and minute for the end time after **until**.

Step 6 Click **OK**.

Backing up Exchange 2010

Backing up Microsoft Exchange 2010 using SonicWALL CDP allows users to store and retrieve Microsoft Exchange revisions from an agent machine. Microsoft Exchange backup cannot be configured using the Web Management Interface.

Note Microsoft Exchange can only be backed up using the Agent User Interface.

See the following sections:

- “Backing Up a User Mailbox” section on page 126
- “Backing Up InfoStore Databases” section on page 133

Backing Up a User Mailbox

You can backup individual user mailboxes by using the Microsoft Exchange User Mailbox Backup and Restore server application in the SonicWALL CDP Agent User Interface. The user mailbox is backed up onto your SonicWALL CDP appliance.

For Microsoft Exchange 2010 on Windows Server 2008, SonicWALL CDP supports backup and restore on a multi-application, single server deployment, in which the same server has several applications installed, such as Exchange, SQL, and Active Directory.

In the Agent User Interface, you can create a **Microsoft Exchange - User Mailbox** application object for for one or more user mailboxes, input the login credentials for the Exchange server, configure a backup schedule, create a backup task, optionally select offsite backup, and restore individual user mailboxes to the Exchange server. For information about restoring a user mailbox, see the “Recovering Exchange 2010 User Mailboxes” section on page 176.

The User Mailbox Backup and Restore feature includes the following capabilities:

- Convenient interface for adding user mailboxes to or deleting them from the backup process
- Ability to set the backup schedule for a group of mailboxes or for individual user mailboxes
- Secure login using credentials to the Microsoft Exchange server
- Optional automatic backup of user mailboxes to an offsite location
- Retention of multiple backups for each user mailbox

User Mailbox Backup and Restore backs up and restores messages in the user’s Outlook Mailbox, including the Inbox, Drafts, Deleted Items, and Sent Items, as well as messages within all other folders with custom names.

It does not back up the Outlook Calendar, Notes, Contacts, Tasks, Meeting Requests, and Public Folders. It also does not back up locally archived folders.

See the following sections:

- “How Does User Mailbox Backup and Restore Work?” section on page 127
- “Adding User Mailboxes to an Application Object” section on page 127
- “Scheduling Backups for User Mailboxes” section on page 129
- “Configuring a Backup Task for User Mailbox Backups” section on page 129
- “Configuring Authentication on the Exchange Server” section on page 130

- "Removing User Mailboxes from the Backup Task" section on page 132
- "Verifying User Mailbox Backup Activity" section on page 132

How Does User Mailbox Backup and Restore Work?

The SonicWALL CDP Microsoft Exchange User Mailbox Backup and Restore feature is implemented as a server application that is automatically discovered by the SonicWALL CDP Agent User Interface. To get started using the feature, select the **Policies** tab and then select **Applications** in the left pane of the Agent User Interface. To backup user mailboxes, you must configure an application object, a schedule, and a backup task that includes both the application object and the schedule.

The User Mailbox application allows you to add or delete individual user mailboxes for backup, set backup schedules, restore specific backups of individual mailboxes, enter credentials for accessing the Exchange server, and configure offsite backup. You can view log entries in the SonicWALL CDP Agent User Interface on the **Status** tab to verify that backups are successful.

Note The SonicWALL CDP appliance must be licensed for server applications. On models that do not support server application licenses, such as the generation 3 SonicWALL CDP 110 and 210, you can still use the User Mailbox Backup and Restore feature.

Adding User Mailboxes to an Application Object

To backup user mailboxes, you must configure an application object, a schedule, and a backup task that includes both the application object and the schedule. This section describes how to create the application object.

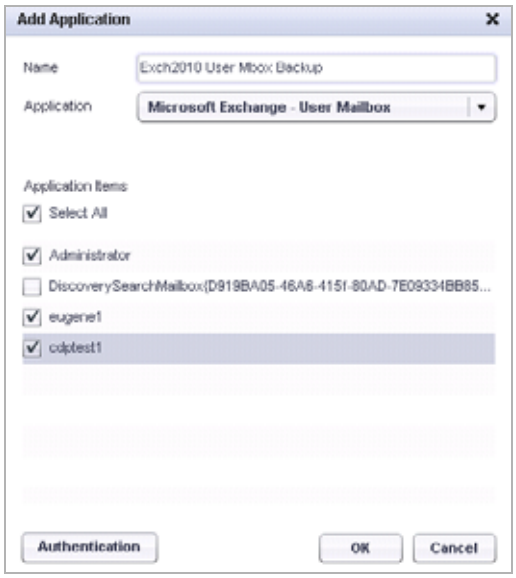
You can test the connection to the Exchange Server by clicking the **Authentication** button while adding or editing an application object. It is not necessary to enter any authentication credentials to test the connection.

To create an application object with individual user mailboxes for backup, perform the following steps:

Step 1 In the SonicWALL CDP Agent User Interface, click the **Policies** tab.

Step 2 In the left pane, click **Applications**.

Step 3 In the right pane, click the Plus button at the lower right corner. The Add Application window opens.

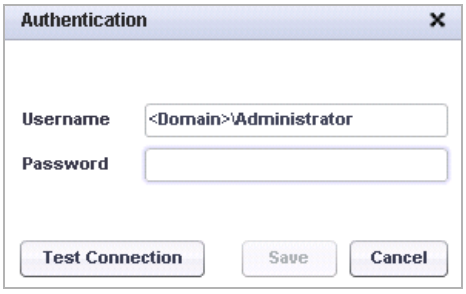


Step 4 Type a descriptive name for the application object into the **Name** field.

Step 5 Select **Microsoft Exchange - User Mailbox** in the **Application** drop-down list. The list of available applications is automatically populated through a discovery process. For proper discovery, the Microsoft Volume Shadow Copy service must not be disabled. See "Backup and Recovery Troubleshooting" on page 229 for more information.

Step 6 Under **Application items**, select the checkboxes for one or more user mailboxes to back up.

Step 7 If authentication credentials are required to access the Exchange server, or to test the connections to the Exchange server, click the **Authentication** button. The Authentication dialog box opens.



Step 8 In the Authentication dialog box, type the domain\username into the **Username** field and type the password into the **Password** field.

Note For Exchange 2010, configure Authentication with ***<your_domain>\Administrator***. When ready to restore a backed up user mailbox, login to the server agent as *Administrator*. For more information, see "Configuring Authentication on the Exchange Server" on page 130.

Step 9 To test the connection between the User Mailbox application and the Exchange server, either with or without credentials, click the **Test Connection** button. If successful, the dialog box displays the message "Connection succeeded."

Step 10 When finished entering the authentication credentials, click **Save**. Click **Cancel** to close the dialog box without saving anything.

Step 11 In the Add Application window, click **OK** to add the application object.

The new application object appears in the **Policies** screen of the Agent User Interface.

Note Before the backup will occur, you must also configure a schedule for this application object, and a backup task that includes both the application object and the schedule.

Scheduling Backups for User Mailboxes

A schedule is required when creating an Application backup task to backup user mailboxes. You can use the same schedule object in more than one backup task.

For instructions on creating a schedule object, see the "Creating Schedules for Application Backups" section on page 124.

Configuring a Backup Task for User Mailbox Backups

A backup task includes both an application object and a schedule for the backup. Without a backup task, no backups will occur.

For offsite backup, you can choose the **Send All Files Offsite** option when adding or editing a backup task.

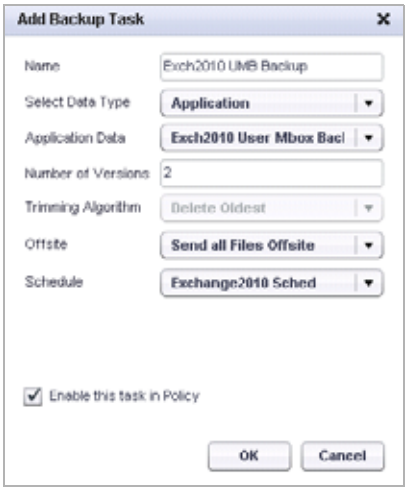
Note Before creating a backup task, create the application object and schedule to be included in the task.

To create a backup task for a user mailbox backup, perform the following steps:

Step 1 In the SonicWALL CDP Agent User Interface, click the **Policies** tab.

Step 2 In the left pane, select **Backup Tasks**.

Step 3 In the right pane, click the Plus button at the lower right corner. The Add Backup Task window opens.



Step 4 Type a descriptive name for the backup task into the **Name** field.

Step 5 Select **Application** from the **Select File Type** drop-down list.

Step 6 Select the desired application object from the **Application Data** drop-down list.

Step 7 Type the desired number of backup revisions to keep into the **Number of Versions** field. The default is 2.

Step 8 The **Trimming Algorithm** field is not configurable for Application policies. The field displays the type of trimming algorithm in use.

Step 9 In the **Offsite** drop-down list, select one of the following options:

- **Send all Files Offsite**
- **Do Not Send Files Offsite**

Step 10 Select the desired schedule from the **Schedule** drop-down list.

Step 11 To activate this backup task, select the **Enable this task in Policy** checkbox. To disable this backup task without deleting it, you can clear this checkbox.

Step 12 Click **OK**.

Configuring Authentication on the Exchange Server

Access between the SonicWALL CDP appliance and the Exchange server where the user mailboxes reside can be configured to require authentication credentials or not. When you add an application object for a user mailbox backup, you can choose to add authentication credentials if required by the Exchange server. In either case, you can use the Authentication dialog box to test the connection between the SonicWALL CDP appliance and the Exchange server.

Note If no authentication credentials are entered, the actual backup process uses the local SYSTEM account to access the Microsoft Exchange database.

Before configuring a User Mailbox application object to use credentials when accessing the Exchange server, you must first configure the credentials on the Exchange server. The user name must have appropriate privileges to access user mailbox data on the Exchange server.

Note For Exchange 2010, configure authentication with ***<your_domain>\Administrator***. When ready to restore a backed up user mailbox, login to the server agent as *Administrator*.

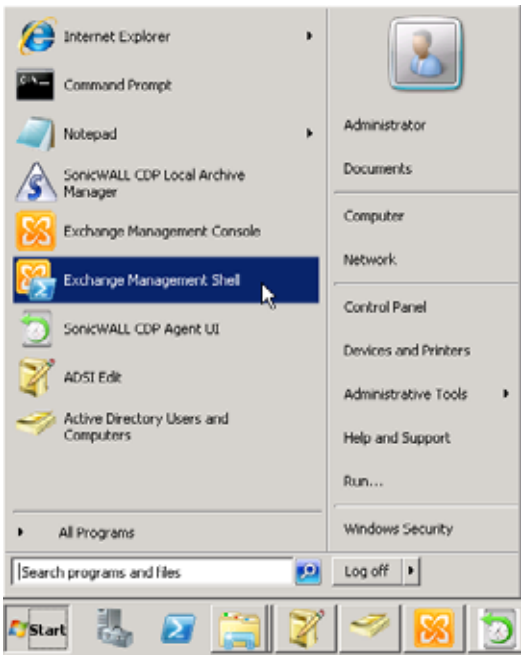
The procedure below provides basic instructions for configuring authentication with the Administrator user. For more information about configuring users and access privileges on Microsoft Exchange, see the following Microsoft knowledge base articles:

http:/support.microsoft.com/kb/821897

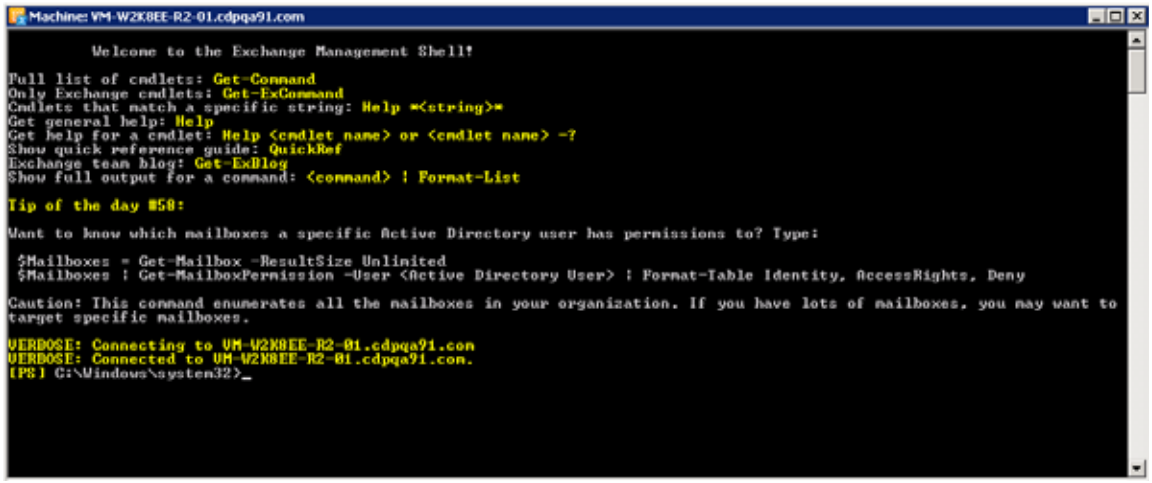
http://support.microsoft.com/kb/556045

To configure the Administrator account for authentication, perform the following steps:

Step 1 Open the Exchange Management Shell on the server.

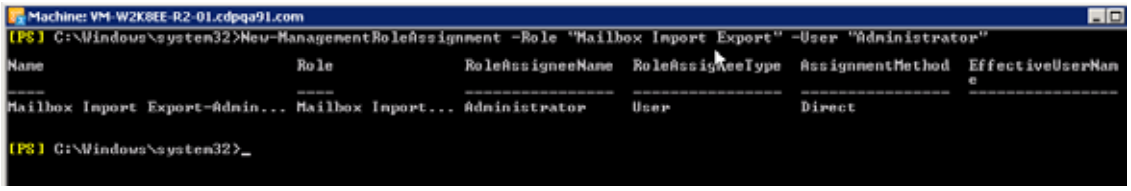


The welcome screen displays, followed by a command prompt.


Machine: VM-W2K8EE-R2-01.cdpqa91.com
Welcome to the Exchange Management Shell!
Full list of cmdlets: Get-Command
Only Exchange cmdlets: Get-ExCommand
Cmdlets that match a specific string: Help *<string>*
Get general help: Help
Get help for a cmdlet: Help <cmdlet name> or <cmdlet name> -?
Show quick reference guide: QuickRef
Exchange team blog: Get-ExBlog
Show full output for a command: <command> | Format-List
Tip of the day #50:
Want to know which mailboxes a specific Active Directory user has permissions to? Type:
$Mailboxes = Get-Mailbox -ResultSize Unlimited
$Mailboxes | Get-MailboxPermission -User <Active Directory User> | Format-Table Identity, AccessRights, Deny
Caution: This command enumerates all the mailboxes in your organization. If you have lots of mailboxes, you may want to target specific mailboxes.
VERBOSE: Connecting to VM-W2K8EE-R2-01.cdpqa91.com
VERBOSE: Connected to VM-W2K8EE-R2-01.cdpqa91.com.
[PS] C:\Windows\system32>

Step 2 Type the following at the prompt:

New–ManagementRoleAssignment –Role “Mailbox Import Export” –User “Administrator”


Machine: VM-W2K8EE-R2-01.cdpqa91.com
[PS] C:\Windows\system32>New-ManagementRoleAssignment -Role "Mailbox Import Export" -User "Administrator"
Name Role RoleAssigneeName RoleAssigneeType AssignmentMethod EffectiveUserName
Mailbox Import Export-Admin... Mailbox Import... Administrator User Direct
[PS] C:\Windows\system32>

Removing User Mailboxes from the Backup Task

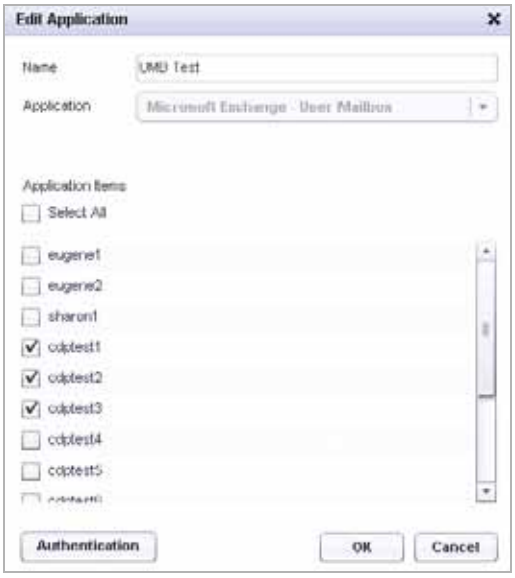
This section describes how to remove a user mailbox from the list of mailboxes scheduled for backup.

To remove a user mailbox from the backup task, perform the following steps:

Step 1 In the SonicWALL CDP Agent User Interface, click the **Policies** tab.

Step 2 In the left pane, select **Applications**.

Step 3 In the right pane, click the Edit button for the application object you wish to edit. The Edit Application window opens.



Step 4 Clear the checkbox for the mailbox you wish to delete.

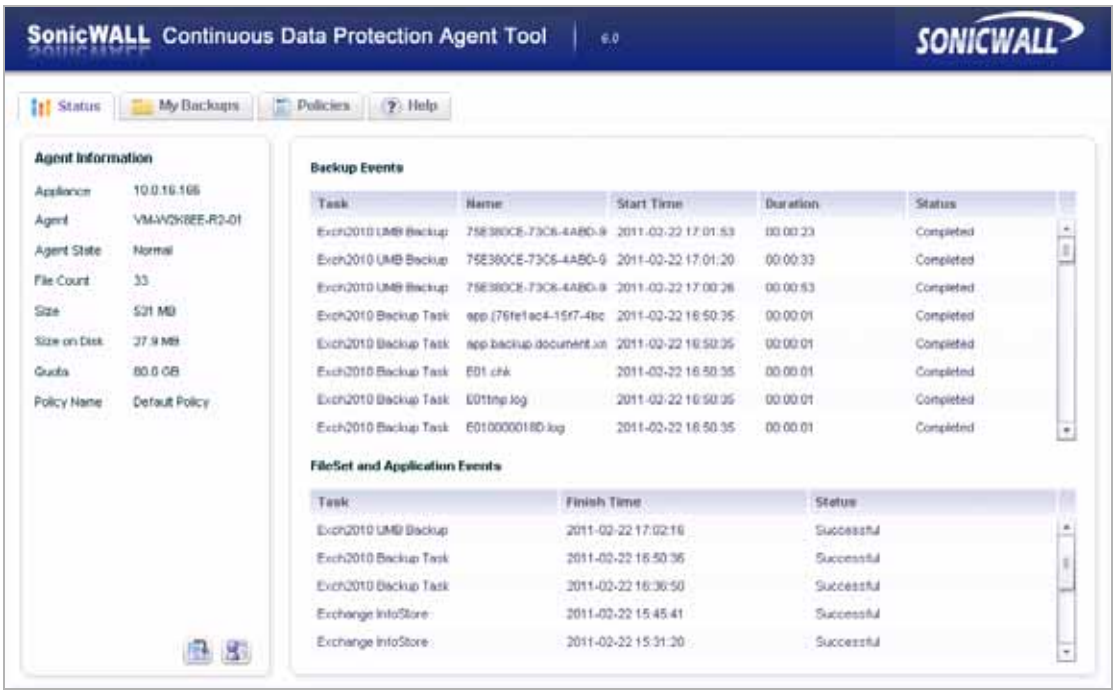
Step 5 Click **OK**.

Verifying User Mailbox Backup Activity

This section describes how to tell if your user mailbox backups are working correctly. You can view log entries showing the backups in the **Status** page of the SonicWALL CDP Agent User Interface.

You should see log entries showing backups right after the first scheduled backup after creating a backup task for one or more user mailboxes, and then after each scheduled backup.

If you are watching the **Status** page during the backup, you will first see the backup task appear multiple times (for each mailbox) in the **Backup Events** table. When all individual backup events are finished, the backup task appears in the **FileSet and Application Events** table as completed.



To verify user mailbox backups:

Step 1 In the SonicWALL CDP Agent User Interface, click the **Status** tab.

Step 2 Optionally, to view backup status on a different appliance, click the change appliance button in the left pane.

Step 3 View the backup status in the right pane.

Backing Up InfoStore Databases

You can backup and restore Microsoft Exchange InfoStore databases by using the SonicWALL CDP Microsoft Exchange InfoStore Backup and Restore server application in the SonicWALL CDP Agent User Interface. The InfoStore databases are backed up onto your SonicWALL CDP appliance.

For Microsoft Exchange 2010 on Windows Server 2008, SonicWALL CDP supports backup and restore on a multi-application, single server deployment, in which the same server has several applications installed, such as Exchange, SQL, and Active Directory.

In the Agent User Interface, you can create a **Microsoft Exchange - InfoStore** application object for for one or more databases, input the login credentials for the Exchange server, configure a backup schedule, create a backup task, optionally select offsite backup, and restore databases back to the Exchange server. For information about restoring InfoStore databases, see the “Recovering Exchange 2010 InfoStore” section on page 179.

Note The SonicWALL CDP appliance must be licensed for server applications. On the SonicWALL CDP 110 or 210 platforms, this feature requires the purchase of a Microsoft Application Server Agent License upgrade. This license allows you to back up any application that is installed on your server, such as Exchange, SQL, Active Directory, SharePoint, or another supported application.

The SonicWALL CDP Microsoft Exchange InfoStore Backup and Restore feature includes the following capabilities:

- Ability to set and manage the backup schedule
- Optional automatic backup to an offsite location
- Retention of multiple backup versions

How Does InfoStore Backup and Restore Work?

The SonicWALL CDP Microsoft Exchange InfoStore Backup and Restore feature is implemented as a server application that is automatically discovered by the SonicWALL CDP Agent User Interface. To get started using the feature, select the **Policies** tab and then select **Applications** in the left pane of the Agent User Interface. To backup Microsoft Exchange databases, you must configure an application object, a schedule, and a backup task that includes both the application object and the schedule.

Note Exchange 2010 InfoStore does not use storage groups, as are used with Exchange 2007/ 2003 InfoStore, but provides direct access to the databases for backup and restore.

The InfoStore application allows you to add or remove individual Microsoft Exchange databases for backup, set backup schedules, restore specific backups of the Exchange server, and configure offsite backup. You can view log entries in the SonicWALL CDP Agent User Interface on the **Status** tab to verify that backups are successful.

For information about supported servers and versions of Exchange, see the "Supported Platforms and Deployment Requirements" section on page 21.

Adding an InfoStore Application Object

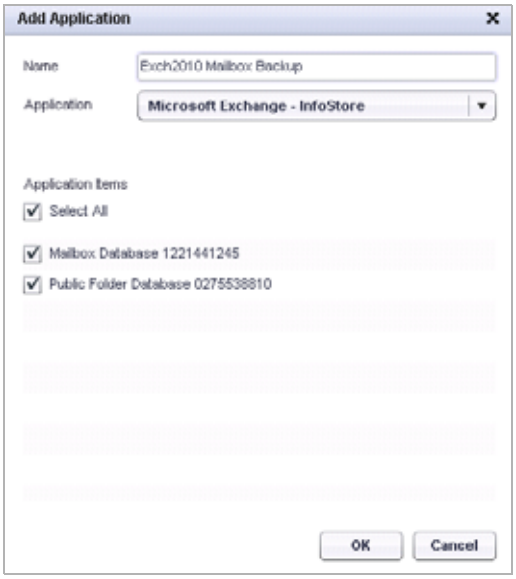
To backup InfoStore databases, you must configure an application object, a schedule, and a backup task that includes both the application object and the schedule. This section describes how to create the application object.

To create an application object for Microsoft Exchange InfoStore backup, perform the following steps:

Step 1 In the SonicWALL CDP Agent User Interface, click the **Policies** tab.

Step 2 In the left pane, click **Applications**.

Step 3 In the right pane, click the Plus button at the lower right corner. The Add Application window opens.



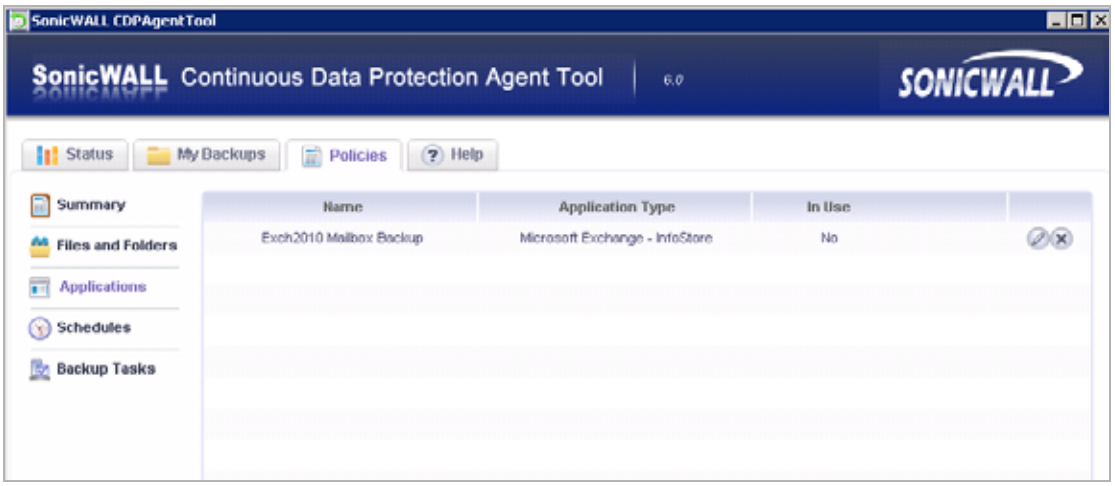
Step 4 Type a descriptive name for the application object into the **Name** field.

Step 5 Select **Microsoft Exchange - InfoStore** in the **Application** drop-down list. The list of available applications is automatically populated through a discovery process. For proper discovery, the Microsoft Volume Shadow Copy and VSS Writer services must not be disabled. See "Backup and Recovery Troubleshooting" on page 229 for more information.

Step 6 Under **Application items**, select the checkboxes for one or more databases to back up. It is not required to back up all databases with the same backup task. For large databases, you might want to schedule separate backups at different times.

Step 7 In the Add Application window, click **OK** to add the application object.

The new application object appears in the **Policies** screen of the Agent User Interface.



Note Before the backup will occur, you must also configure a schedule for this application object, and a backup task that includes both the application object and the schedule.

Scheduling Backups for InfoStore

A schedule is required when creating an Application backup task to backup InfoStore databases. You can use the same schedule object in more than one backup task.

For instructions on creating a schedule object, see the "Creating Schedules for Application Backups" section on page 124.

Configuring a Backup Task for InfoStore Backups

A backup task includes both an application object and a schedule for the backup. Without a backup task, no backups will occur.

For offsite backup, you can choose the **Send All Files Offsite** option when adding or editing a backup task.

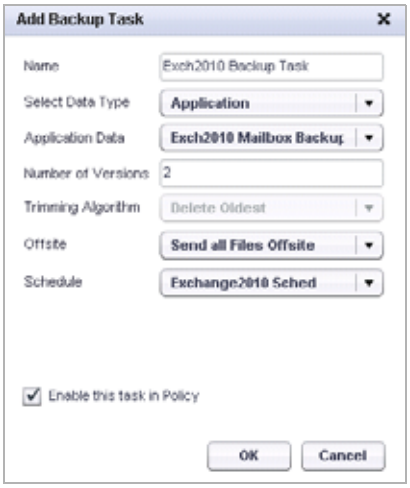
Note Before creating a backup task, create the application object and schedule to be included in the task.

To create a backup task for an InfoStore backup, perform the following steps:

Step 1 In the SonicWALL CDP Agent User Interface, click the **Policies** tab.

Step 2 In the left pane, select **Backup Tasks**.

Step 3 In the right pane, click the Plus button at the lower right corner. The Add Backup Task window opens.



Step 4 Type a descriptive name for the backup task into the **Name** field.

Step 5 Select **Application** from the **Select File Type** drop-down list.

Step 6 Select the desired application object from the **Application Data** drop-down list.

Step 7 Type the desired number of backup revisions to keep into the **Number of Versions** field. The default is 2.

Step 8 The **Trimming Algorithm** field is not configurable for Application policies. The field displays the type of trimming algorithm in use.

Step 9 In the **Offsite** drop-down list, select one of the following options:

- **Send all Files Offsite** – Offsite backup settings must already be configured in the SonicWALL CDP Web Management Interface, and the offsite appliance must be available.
- **Do Not Send Files Offsite** – No files will be sent offsite.

Step 10 Select the desired schedule from the **Schedule** drop-down list.

Step 11 To activate this backup task, select the **Enable this task in Policy** checkbox. To disable this backup task without deleting it, you can clear this checkbox.

Step 12 Click **OK**.

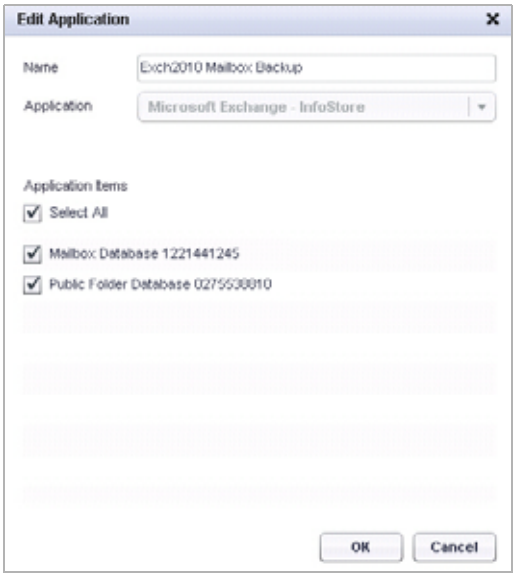
Removing a Database from the Backup Task

To remove a storage group from the list of groups scheduled for backup, perform the following steps:

Step 1 In the SonicWALL CDP Agent User Interface, click the **Policies** tab.

Step 2 In the left pane, select **Applications**.

Step 3 In the right pane, click the Edit button for the application object you wish to edit. The Edit Application window opens.



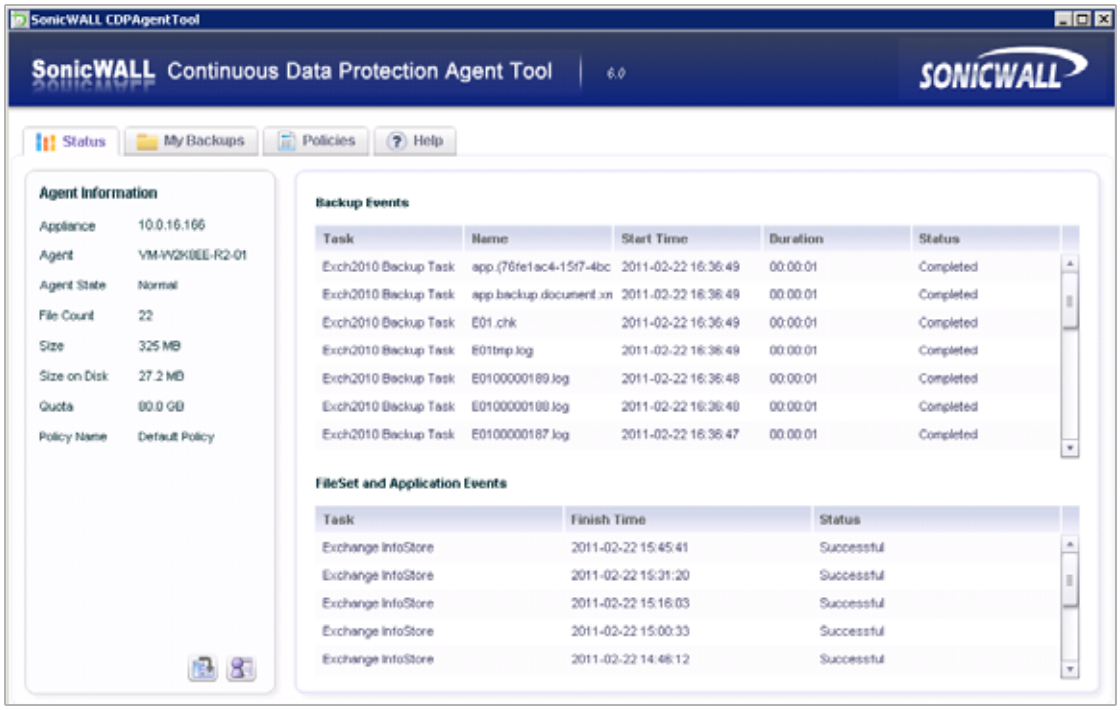
Step 4 Clear the checkbox for the database you wish to delete.

Step 5 Click **OK**.

Verifying InfoStore Backup Activity

This section describes how to tell if your Microsoft Exchange backups are working correctly. You can view log entries showing the backups in the **Status** page of the SonicWALL CDP Agent User Interface.

You should see log entries showing backups after each scheduled backup after creating a backup task for one or more InfoStore databases. If you are watching the **Status** page during the backup, you will first see the backup task appear multiple times in the **Backup Events** table. When all individual backup events are finished, the backup task appears in the **FileSet and Application Events** table as completed.


SonicWALL CDPAgentTool
SonicWALL Continuous Data Protection Agent Tool
6.0
SONICWALL
Status
My Backups
Policies
Help
Agent Information
Appliance 10.0.16.166
Agent VM-W2K8EE-R2-01
Agent State Normal
File Count 22
Size 325 MB
Size on Disk 27.2 MB
Quota 80.0 GB
Policy Name Default Policy
Backup Events
Task Name Start Time Duration Status
Exch2010 Backup Task app.{76fe1ac4-15f7-4bc 2011-02-22 16:36:49 00:00:01 Completed
Exch2010 Backup Task app.backup.document.xn 2011-02-22 16:36:49 00:00:01 Completed
Exch2010 Backup Task E01.chk 2011-02-22 16:36:49 00:00:01 Completed
Exch2010 Backup Task E01tmp.log 2011-02-22 16:36:49 00:00:01 Completed
Exch2010 Backup Task E0100000189.log 2011-02-22 16:36:48 00:00:01 Completed
Exch2010 Backup Task E0100000188.log 2011-02-22 16:36:48 00:00:01 Completed
Exch2010 Backup Task E0100000187.log 2011-02-22 16:36:47 00:00:01 Completed
FileSet and Application Events
Task Finish Time Status
Exchange InfoStore 2011-02-22 15:45:41 Successful
Exchange InfoStore 2011-02-22 15:31:20 Successful
Exchange InfoStore 2011-02-22 15:16:03 Successful
Exchange InfoStore 2011-02-22 15:00:33 Successful
Exchange InfoStore 2011-02-22 14:46:12 Successful

To verify an InfoStore backup:

Step 1 In the SonicWALL CDP Agent User Interface, click the **Status** tab.

Step 2 Optionally, to view backup status on a different appliance, click the change appliance button in the left pane. This only applies if the agent has previously backed up files on a different appliance.

Step 3 View the backup status in the right pane.

Backing up Exchange 2007/2003

Backing up Microsoft Exchange 2007 or 2003 using SonicWALL CDP allows users to store and retrieve Microsoft Exchange revisions from an agent machine. Microsoft Exchange backup cannot be configured using the Web Management Interface.

Note Microsoft Exchange can only be backed up using the Agent User Interface.

See the following sections:

- “Backing Up a User Mailbox” section on page 139
- “Backing Up a Storage Group” section on page 145

Backing Up a User Mailbox

You can backup individual user mailboxes by using the Microsoft Exchange User Mailbox Backup and Restore server application in the SonicWALL CDP Agent User Interface. The user mailbox is backed up onto your SonicWALL CDP appliance.

For Microsoft Exchange 2010 on Windows Server 2008, SonicWALL CDP supports backup and restore on a multi-application, single server deployment, in which the same server has several applications installed, such as Exchange, SQL, and Active Directory.

In the Agent User Interface, you can create a **Microsoft Exchange - User Mailbox** application object for for one or more user mailboxes, input the login credentials for the Exchange server, configure a backup schedule, create a backup task, optionally select offsite backup, and restore individual user mailboxes to the Exchange server. For information about restoring a user mailbox, see the “Recovering an Exchange 2007/2003 User Mailbox” section on page 181.

The User Mailbox Backup and Restore feature includes the following capabilities:

- Convenient interface for adding user mailboxes to or deleting them from the backup process
- Ability to set the backup schedule for a group of mailboxes or for individual user mailboxes
- Secure login using credentials to the Microsoft Exchange server
- Optional automatic backup of user mailboxes to an offsite location
- Retention of multiple backups for each user mailbox

User Mailbox Backup and Restore backs up and restores messages in the user’s Outlook Mailbox, including the Inbox, Drafts, Deleted Items, and Sent Items, as well as messages within all other folders with custom names.

It does not back up the Outlook Calendar, Notes, Contacts, Tasks, Meeting Requests, and Public Folders. It also does not back up locally archived folders.

See the following sections:

- “How Does User Mailbox Backup and Restore Work?” section on page 140
- “Installation Prerequisites” section on page 140
- “Adding User Mailboxes to an Application Object” section on page 141
- “Scheduling Backups for User Mailboxes” section on page 142
- “Configuring a Backup Task for User Mailbox Backups” section on page 142
- “Configuring and Testing Access to the Exchange Server” section on page 143

- "Removing User Mailboxes from the Backup Task" section on page 144
- "Verifying User Mailbox Backup Activity" section on page 144

How Does User Mailbox Backup and Restore Work?

The SonicWALL CDP Microsoft Exchange User Mailbox Backup and Restore feature is implemented as a server application that is automatically discovered by the SonicWALL CDP Agent User Interface. To get started using the feature, select the **Policies** tab and then select **Applications** in the left pane of the Agent User Interface. To backup user mailboxes, you must configure an application object, a schedule, and a backup task that includes both the application object and the schedule.

The User Mailbox application allows you to add or delete individual user mailboxes for backup, set backup schedules, restore specific backups of individual mailboxes, enter credentials for accessing the Exchange server, and configure offsite backup. You can view log entries in the SonicWALL CDP Agent User Interface on the **Status** tab to verify that backups are successful.

Installation Prerequisites

This section lists the necessary prerequisites for successful operation of the SonicWALL CDP Agent User Interface with the Microsoft Exchange User Mailbox Backup and Restore feature. For information about supported servers and versions of Exchange, see the "Supported Platforms and Deployment Requirements" section on page 21.

Note The SonicWALL CDP appliance must be licensed for server applications. On models that do not support server application licenses, such as SonicWALL CDP 110 and 210, you can still use the User Mailbox Backup and Restore feature.

ExOLEDB / ADO / CDO Requirements for Exchange 2007/2003/2000

SonicWALL CDP uses **ExOLEDB** to access Microsoft Exchange 2007, 2003, and 2000. The **Exchange OLE DB Provider** should be installed along with Microsoft Exchange, and must be accessible by the SonicWALL CDP Web Management Interface and Agent User Interface.

The ADO (ActiveX Data Objects) and CDO (Collaboration Data Objects) APIs are also required by this feature. These are application programming interfaces provided by Microsoft that allow applications to access data stores in a uniform manner. These APIs are included with the Microsoft Exchange installation.

Note This requirement does not apply to Exchange 2010.

ESE Backup Client DLL/ CDOEXM Requirements for Legacy Exchange

SonicWALL CDP uses the Exchange Backup and Restore API to access Microsoft Exchange. The Microsoft ESE Backup Client DLL (EsEbCli2.dll) should be installed along with Microsoft Exchange, and must be accessible by SonicWALL CDP Web Management Interface and Agent User Interface. The Collaboration Data Objects for Exchange Management (CDOEXM) APIs are also used to automate the restore procedure, but not required by this feature.

Note This requirement only applies for Exchange backups created on SonicWALL CDP 5.1 or earlier.

Adding User Mailboxes to an Application Object

To backup user mailboxes, you must configure an application object, a schedule, and a backup task that includes both the application object and the schedule. This section describes how to create the application object.

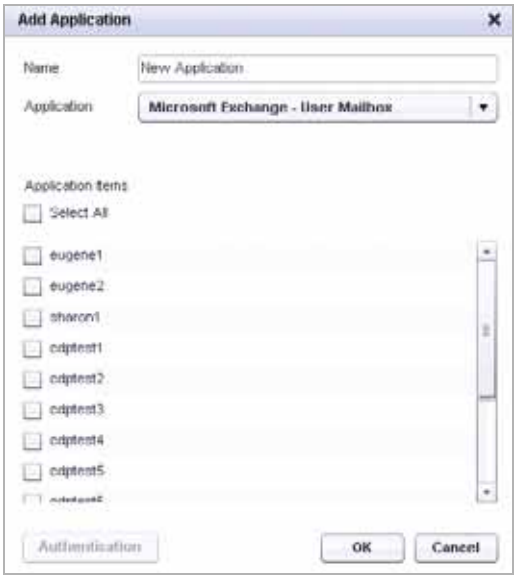
You can test the connection to the Exchange Server by clicking the **Authentication** button while adding or editing an application object. It is not necessary to enter any authentication credentials to test the connection.

To create an application object with individual user mailboxes for backup, perform the following steps:

Step 1 In the SonicWALL CDP Agent User Interface, click the **Policies** tab.

Step 2 In the left pane, click **Applications**.

Step 3 In the right pane, click the Plus button at the lower right corner. The Add Application window opens.



Step 4 Type a descriptive name for the application object into the **Name** field.

Step 5 Select **Microsoft Exchange - User Mailbox** in the **Application** drop-down list. The list of available applications is automatically populated through a discovery process. For proper discovery, the Microsoft Volume Shadow Copy service must not be disabled. See "Backup and Recovery Troubleshooting" on page 229 for more information.

Step 6 Under **Application items**, select the checkboxes for one or more user mailboxes to back up.

Step 7 If authentication credentials are required to access the Exchange server, or to test the connections to the Exchange server, click the **Authentication** button. The Authentication dialog box opens.

Step 8 In the Authentication dialog box, type the domain\username into the **Username** field and type the password into the **Password** field.

Note For Exchange 2007/2003, configure Authentication with ***<your_domain>\cdpAdmin***. When ready to restore a backed up user mailbox, login to the server agent as *cdpAdmin*.

Step 9 To test the connection between the User Mailbox application and the Exchange server, either with or without credentials, click the **Test Connection** button.

Step 10 When finished entering the authentication credentials, click **Save**. Click **Cancel** to close the dialog box without saving anything.

Step 11 In the Add Application window, click **OK** to add the application object.

The new application object appears in the **Policies** screen of the Agent User Interface.

Note Before the backup will occur, you must also configure a schedule for this application object, and a backup task that includes both the application object and the schedule.

Scheduling Backups for User Mailboxes

A schedule is required when creating an Application backup task to backup user mailboxes. You can use the same schedule object in more than one backup task.

For instructions on creating a schedule object, see the "Creating Schedules for Application Backups" section on page 124.

Configuring a Backup Task for User Mailbox Backups

A backup task includes both an application object and a schedule for the backup. Without a backup task, no backups will occur.

For offsite backup, you can choose the **Send All Files Offsite** option when adding or editing a backup task.

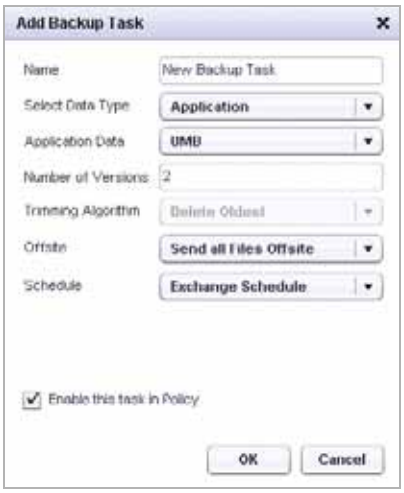
Note Before creating a backup task, create the application object and schedule to be included in the task.

To create a backup task for a user mailbox backup, perform the following steps:

Step 1 In the SonicWALL CDP Agent User Interface, click the **Policies** tab.

Step 2 In the left pane, select **Backup Tasks**.

Step 3 In the right pane, click the Plus button at the lower right corner. The Add Backup Task window opens.



Step 4 Type a descriptive name for the backup task into the **Name** field.

Step 5 Select **Application** from the **Select File Type** drop-down list.

Step 6 Select the desired application object from the **Application Data** drop-down list.

Step 7 Type the desired number of backup revisions to keep into the **Number of Versions** field. The default is 2.

Step 8 The **Trimming Algorithm** field is not configurable for Application policies. The field displays the type of trimming algorithm in use.

Step 9 In the **Offsite** drop-down list, select one of the following options:

- **Send all Files Offsite**
- **Do Not Send Files Offsite**

Step 10 Select the desired schedule from the **Schedule** drop-down list.

Step 11 To activate this backup task, select the **Enable this task in Policy** checkbox. To disable this backup task without deleting it, you can clear this checkbox.

Step 12 Click **OK**.

Configuring and Testing Access to the Exchange Server

Access between the SonicWALL CDP appliance and the Exchange server where the user mailboxes reside can be configured to require authentication credentials or not. When you add an application object for a user mailbox backup, you can choose to add authentication credentials if required by the Exchange server. In either case, you can use the Authentication dialog box to test the connection between the SonicWALL CDP appliance and the Exchange server.

Note If no authentication credentials are entered, the actual backup process uses the local SYSTEM account to access the Microsoft Exchange database.

Before configuring a User Mailbox application object to use credentials when accessing the Exchange server, you must first configure the credentials on the Exchange server. The user name must have appropriate privileges to access user mailbox data on the Exchange server. For more information about configuring users and access privileges on Microsoft Exchange, see the following Microsoft knowledge base articles:

http:/support.microsoft.com/kb/821897

http://support.microsoft.com/kb/556045

Removing User Mailboxes from the Backup Task

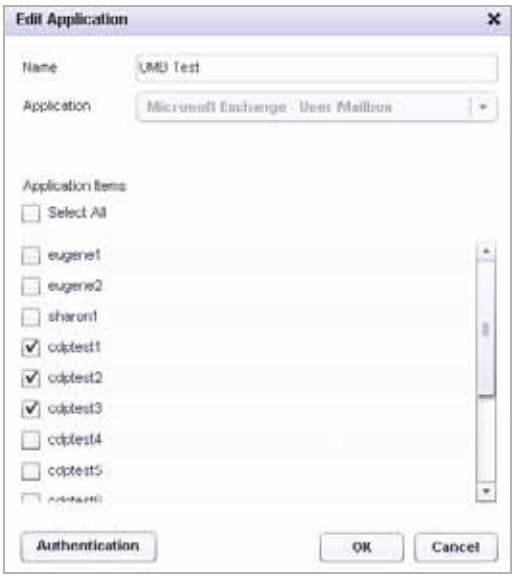
This section describes how to remove a user mailbox from the list of mailboxes scheduled for backup.

To remove a user mailbox from the backup task, perform the following steps:

Step 1 In the SonicWALL CDP Agent User Interface, click the **Policies** tab.

Step 2 In the left pane, select **Applications**.

Step 3 In the right pane, click the Edit button for the application object you wish to edit. The Edit Application window opens.



Step 4 Clear the checkbox for the mailbox you wish to delete.

Step 5 Click **OK**.

Verifying User Mailbox Backup Activity

This section describes how to tell if your user mailbox backups are working correctly. You can view log entries showing the backups in the **Status** page of the SonicWALL CDP Agent User Interface.

You should see log entries showing backups right after the first scheduled backup after creating a backup task for one or more user mailboxes, and then after each scheduled backup.

Step 1 In the SonicWALL CDP Agent User Interface, click the **Status** tab.

Step 2 Optionally, to view backup status on a different appliance, click the change appliance button in the left pane.

Step 3 View the backup status in the right pane.

Backing Up a Storage Group

You can backup and restore a Microsoft Exchange Storage Group by using the SonicWALL CDP Microsoft Exchange InfoStore Backup and Restore server application in the SonicWALL CDP Agent User Interface. The Storage Group, or InfoStore, is backed up onto your SonicWALL CDP appliance.

For Microsoft Exchange 2010 on Windows Server 2008, SonicWALL CDP supports backup and restore on a multi-application, single server deployment, in which the same server has several applications installed, such as Exchange, SQL, and Active Directory.

In the Agent User Interface, you can create a **Microsoft Exchange - InfoStore** application object for for one or more storage groups, input the login credentials for the Exchange server, configure a backup schedule, create a backup task, optionally select offsite backup, and restore storage groups back to the Exchange server. For information about restoring a Storage Group, see the "Recovering an Exchange 2007/2003 Storage Group" section on page 184.

Note The SonicWALL CDP appliance must be licensed for server applications. On the SonicWALL CDP 110 and 210 platforms, this feature requires the purchase of the SonicWALL CDP 110/210 5 Server Applications License upgrade. This license allows you to back up five applications that are installed on your server, such as Exchange, SQL, Active Directory, and others.

The SonicWALL CDP Microsoft Exchange InfoStore Backup and Restore feature includes the following capabilities:

- Ability to set and manage the backup schedule
- Optional automatic backup to an offsite location
- Retention of multiple backup versions

How Does InfoStore Backup and Restore Work?

The SonicWALL CDP Microsoft Exchange InfoStore Backup and Restore feature is implemented as a server application that is automatically discovered by the SonicWALL CDP Agent User Interface. To get started using the feature, select the **Policies** tab and then select **Applications** in the left pane of the Agent User Interface. To backup a storage group, you must configure an application object, a schedule, and a backup task that includes both the application object and the schedule.

The InfoStore application allows you to add or remove individual Microsoft Exchange Storage Groups for backup, set backup schedules, restore specific backups of the Exchange server, and configure offsite backup. You can view log entries in the SonicWALL CDP Agent User Interface on the **Status** tab to verify that backups are successful.

Installation Prerequisites

This section lists the necessary prerequisites for successful operation of the **Microsoft Exchange - InfoStore** server application on the SonicWALL CDP Agent User Interface. For information about supported servers and versions of Exchange, see the "Supported Platforms and Deployment Requirements" section on page 21.

ESE Backup Client DLL/ CDOEXM Requirements

SonicWALL CDP uses the Exchange Backup and Restore API to access Microsoft Exchange. The Microsoft ESE Backup Client DLL (EsEbCli2.dll) should be installed along with Microsoft Exchange, and must be accessible by SonicWALL CDP Web Management Interface and Agent User Interface. The Collaboration Data Objects for Exchange Management (CDOEXM) APIs are also used to automate the restore procedure, but not required by this feature.

You can copy the EsEbCli2.dll file from your Microsoft installation disk, or download it from Microsoft, or copy it manually from another location into the SonicWALL Continuous Data Protection folder where the Agent client was installed. The default program installation folder location is:

C:\Program Files\SonicWALL\SonicWALL Continuous Data Protection

Note Version 8.1.240.3 of EsEbcli2.dll is required by SonicWALL CDP.

Adding a Storage Group Application Object

To backup a storage group, you must configure an application object, a schedule, and a backup task that includes both the application object and the schedule. This section describes how to create the application object.

To create an application object for Microsoft Exchange Storage Group backup, perform the following steps:

Step 1 In the SonicWALL CDP Agent User Interface, click the **Policies** tab.

Step 2 In the left pane, click **Applications**.

Step 3 In the right pane, click the Plus button at the lower right corner. The Add Application window opens.

Step 4 Type a descriptive name for the application object into the **Name** field.

Step 5 Select **Microsoft Exchange - InfoStore** in the **Application** drop-down list. The list of available applications is automatically populated through a discovery process. For proper discovery, the Microsoft Volume Shadow Copy and VSS Writer services must not be disabled. See "Backup and Recovery Troubleshooting" on page 229 for more information.

Step 6 Under **Application items**, select the checkboxes for one or more storage groups to back up.

Step 7 In the Add Application window, click **OK** to add the application object.

The new application object appears in the **Policies** screen of the Agent User Interface.

Note Before the backup will occur, you must also configure a schedule for this application object, and a backup task that includes both the application object and the schedule.

Scheduling Backups for Storage Groups

A schedule is required when creating an Application backup task to backup a storage group. You can use the same schedule object in more than one backup task.

For instructions on creating a schedule object, see the "Creating Schedules for Application Backups" section on page 124.

Configuring a Backup Task for Storage Group Backups

A backup task includes both an application object and a schedule for the backup. Without a backup task, no backups will occur.

For offsite backup, you can choose the **Send All Files Offsite** option when adding or editing a backup task.

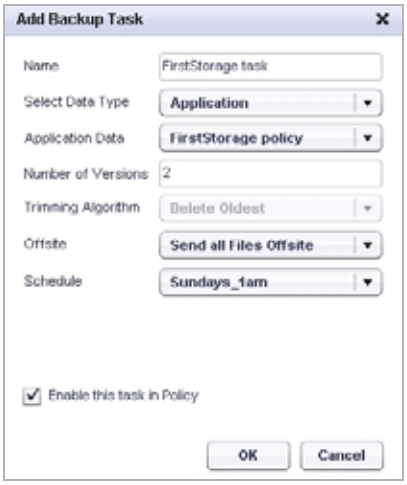
Note Before creating a backup task, create the application object and schedule to be included in the task.

To create a backup task for a storage group backup, perform the following steps:

Step 1 In the SonicWALL CDP Agent User Interface, click the **Policies** tab.

Step 2 In the left pane, select **Backup Tasks**.

Step 3 In the right pane, click the Plus button at the lower right corner. The Add Backup Task window opens.



Step 4 Type a descriptive name for the backup task into the **Name** field.

Step 5 Select **Application** from the **Select File Type** drop-down list.

Step 6 Select the desired application object from the **Application Data** drop-down list.

Step 7 Type the desired number of backup revisions to keep into the **Number of Versions** field. The default is 2.

Step 8 The **Trimming Algorithm** field is not configurable for Application policies. The field displays the type of trimming algorithm in use.

Step 9 In the **Offsite** drop-down list, select one of the following options:

- **Send all Files Offsite** – Offsite backup settings must already be configured in the SonicWALL CDP Web Management Interface, and the offsite appliance must be available.
- **Do Not Send Files Offsite** – No files will be sent offsite.

Step 10 Select the desired schedule from the **Schedule** drop-down list.

Step 11 To activate this backup task, select the **Enable this task in Policy** checkbox. To disable this backup task without deleting it, you can clear this checkbox.

Step 12 Click **OK**.

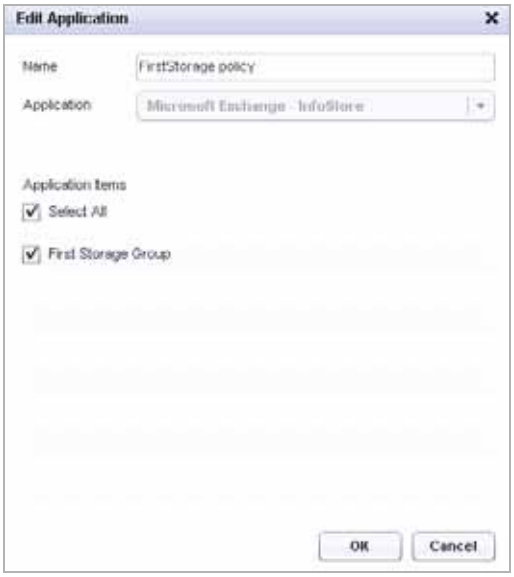
Removing a Storage Group from the Backup Task

To remove a storage group from the list of groups scheduled for backup, perform the following steps:

Step 1 In the SonicWALL CDP Agent User Interface, click the **Policies** tab.

Step 2 In the left pane, select **Applications**.

Step 3 In the right pane, click the Edit button for the application object you wish to edit. The Edit Application window opens.



Step 4 Clear the checkbox for the storage group you wish to delete.

Step 5 Click **OK**.

Verifying InfoStore Backup Activity

This section describes how to tell if your Microsoft Exchange backups are working correctly. You can view log entries showing the backups in the **Status** page of the SonicWALL CDP Agent User Interface.

You should see log entries showing backups after each scheduled backup after creating a backup task for one or more storage groups.

Step 1 In the SonicWALL CDP Agent User Interface, click the **Status** tab.

Step 2 Optionally, to view backup status on a different appliance, click the change appliance button in the left pane. This only applies if the agent has previously backed up files on a different appliance.

Step 3 View the backup status in the right pane.

Obtaining EsEbcli2.dll from the Microsoft Exchange Server 2007 Installation CD

This section describes how to manually obtain the EsEbcli2.dll from your Microsoft Exchange Server 2007 Installation CD.

Step 1 Navigate to setup\i386\exchange\bin folder of the Exchange 2007 installation CD

Step 2 Locate version 8.1.240.3 of the EsEbcli2.dll file, right-click it and select **Copy** from the pop up menu.

Step 3 Navigate to C:\Program Files(x86)\SonicWALL\SonicWALL Continuous Data Protection\ folder on your machine.

Step 4 Right-click inside the folder and select **Paste** from the pop up menu.

Step 5 Restart the CDP Agent User Interface and the SonicWALL CDP Agent Service.

The Microsoft Exchange - InfoStore application should function properly.

Obtaining EsEbcli2.dll from the Microsoft Download Center

This section describes how to manually obtain the EsEbcli2.dll from the Microsoft Exchange Server 2007 Service Pack 1, available at the Microsoft Download Center.

Step 1 Navigate to Microsoft Download Center at <http://www.microsoft.com/downloads>.

Step 2 Type in “E2K7SP1EN32.exe” in the search window and select **Go**.

Step 3 List of results will appear. Select the **Exchange Server 2007 Service Pack 1** page.

Step 4 Scroll down to the bottom of the page and select the **Download** button next to E2K7SP1EN32.exe file. Make sure to download the 32-bit version, the 64-bit version does not include the missing DLL file.

Step 5 Extract the E2K7SP1EN32.exe file, making sure to note down the extraction folder.

Step 6 Navigate to the extraction folder from step 3 and to the following path <setup\serverroles\common\path> inside the folder.

Step 7 Locate version 8.1.240.3 of the EsEbcli2.dll file, right-click it and select **Copy** from the pop up menu.

Step 8 Navigate to C:\Program Files(x86)\SonicWALL\SonicWALL Continuous Data Protection\ folder.

Step 9 Right-click inside the folder and select **Paste** from the pop up menu.

Step 10 Restart the CDP Agent User Interface and the SonicWALL CDP Agent Service.

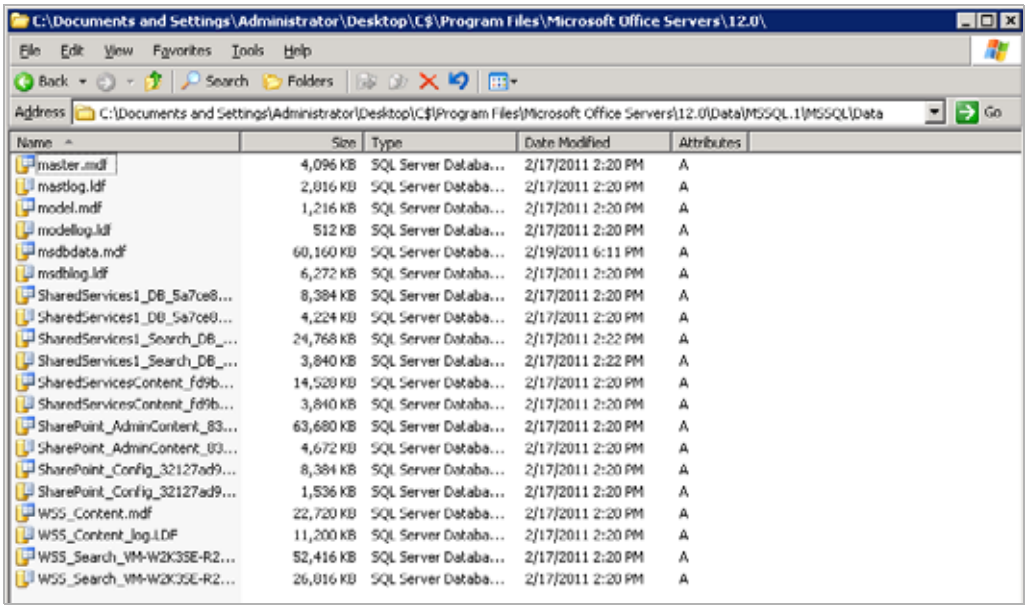
The Microsoft Exchange - InfoStore application should function properly.

Backing Up SharePoint

Backing up Microsoft SharePoint using SonicWALL CDP allows users to store and retrieve SharePoint database revisions from an agent machine. SharePoint databases are configured for backup using the SonicWALL CDP Agent User Interface.

Note SharePoint backup can only be configured using the Agent User Interface.

The application used for SharePoint backup is **Microsoft SQL Server/SharePoint**, as SharePoint uses Microsoft SQL databases. The default SQL master, model, and msdb databases are required for SharePoint, and SharePoint creates other SQL databases as well. Microsoft SQL can be installed on the same or on another Windows Server machine.


C:\Documents and Settings\Administrator\Desktop\C$\Program Files\Microsoft Office Servers\12.0\
File Edit View Favorites Tools Help
Back Search Folders
Address C:\Documents and Settings\Administrator\Desktop\C$\Program Files\Microsoft Office Servers\12.0\Data\MSSQL.1\MSSQL\Data
Go
Name Size Type Date Modified Attributes
master.mdf 4,096 KB SQL Server Databa... 2/17/2011 2:20 PM A
mastlog.ldf 2,016 KB SQL Server Databa... 2/17/2011 2:20 PM A
model.mdf 1,216 KB SQL Server Databa... 2/17/2011 2:20 PM A
modellog.ldf 512 KB SQL Server Databa... 2/17/2011 2:20 PM A
msdbdata.mdf 60,160 KB SQL Server Databa... 2/19/2011 6:11 PM A
msdblog.ldf 6,272 KB SQL Server Databa... 2/17/2011 2:20 PM A
SharedServices1_DB_5a7ce8... 8,384 KB SQL Server Databa... 2/17/2011 2:20 PM A
SharedServices1_DB_5a7ce8... 4,224 KB SQL Server Databa... 2/17/2011 2:20 PM A
SharedServices1_Search_DB_... 24,768 KB SQL Server Databa... 2/17/2011 2:22 PM A
SharedServices1_Search_DB_... 3,840 KB SQL Server Databa... 2/17/2011 2:22 PM A
SharedServicesContent_fd9b... 14,528 KB SQL Server Databa... 2/17/2011 2:20 PM A
SharedServicesContent_fd9b... 3,840 KB SQL Server Databa... 2/17/2011 2:20 PM A
SharePoint_AdminContent_83... 63,680 KB SQL Server Databa... 2/17/2011 2:20 PM A
SharePoint_AdminContent_83... 4,672 KB SQL Server Databa... 2/17/2011 2:20 PM A
SharePoint_Config_32127ad9... 8,384 KB SQL Server Databa... 2/17/2011 2:20 PM A
SharePoint_Config_32127ad9... 1,536 KB SQL Server Databa... 2/17/2011 2:20 PM A
WSS_Content.mdf 22,720 KB SQL Server Databa... 2/17/2011 2:20 PM A
WSS_Content_log.LDF 11,200 KB SQL Server Databa... 2/17/2011 2:20 PM A
WSS_Search_VM-W2K3SE-R2... 52,416 KB SQL Server Databa... 2/17/2011 2:20 PM A
WSS_Search_VM-W2K3SE-R2... 26,816 KB SQL Server Databa... 2/17/2011 2:20 PM A

SonicWALL recommends backing up all SharePoint databases together, rather than backing up individual databases separately.

For information about restoring SharePoint databases, see the "Recovering SharePoint" section on page 189.

See the following sections for SharePoint backup procedures:

- "Creating an Application Object for SharePoint" section on page 151
- "Scheduling Backups for SharePoint" section on page 152
- "Configuring a Backup Task for SharePoint" section on page 153
- "Verifying SharePoint Backup Activity" section on page 154

Creating an Application Object for SharePoint

To backup Microsoft SharePoint, you must configure an application object, a schedule, and a backup task that includes both the application object and the schedule. This section describes how to create the application object.

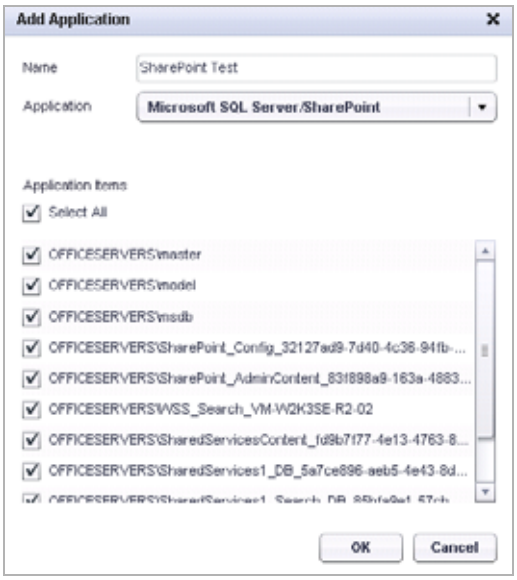
To backup SharePoint using the Agent User Interface, perform the following steps:

Step 1 Open the **SonicWALL Agent User Interface** on the SharePoint server.

Step 2 In the SonicWALL CDP Agent User Interface, click the **Policies** tab.

Step 3 In the left pane, click **Applications**.

Step 4 In the right pane, click the Plus button at the lower right corner. The Add Application window opens.



Step 5 Type a descriptive name for the application object into the **Name** field.

Step 6 Select **Microsoft SQL Server/SharePoint** in the **Application** drop-down list. The list of available applications is automatically populated through a discovery process. For proper discovery, the Microsoft Volume Shadow Copy service must not be disabled. See "Backup and Recovery Troubleshooting" on page 229 for more information.

Step 7 Under **Application items**, select the checkboxes for one or more SharePoint databases to back up. SonicWALL recommends selecting the **Select All** checkbox to ensure that all associated files are backed up for SharePoint.

Step 8 In the Add Application window, click **OK** to add the application object.

The new application object appears in the **Policies** screen of the Agent User Interface.

Note Before the backup will occur, you must also configure a schedule for this application object, and a backup task that includes both the application object and the schedule.

Scheduling Backups for SharePoint

A schedule is required when creating an Application backup task to backup Microsoft SharePoint. You can use the same schedule object in more than one backup task.

For instructions on creating a schedule object, see the "Creating Schedules for Application Backups" section on page 124.

Configuring a Backup Task for SharePoint

A backup task includes both an application object and a schedule for the backup. Without a backup task, no backups will occur.

For offsite backup, you can choose the **Send All Files Offsite** option when adding or editing a backup task.

Note Before creating a backup task, create the application object and schedule to be included in the task.

To create a backup task for a SharePoint backup, perform the following steps:

Step 1 In the SonicWALL CDP Agent User Interface, click the **Policies** tab.

Step 2 In the left pane, select **Backup Tasks**.

Step 3 In the right pane, click the Plus button at the lower right corner. The Add Backup Task window opens.

Step 4 Type a descriptive name for the backup task into the **Name** field.

Step 5 Select **Application** from the **Select File Type** drop-down list.

Step 6 Select the desired application object from the **Application Data** drop-down list.

Step 7 Type the desired number of backup revisions to keep into the **Number of Versions** field. The default is 2.

Step 8 The **Trimming Algorithm** field is not configurable for Application policies. The field displays the type of trimming algorithm in use.

Step 9 In the **Offsite** drop-down list, select one of the following options:

- **Send all Files Offsite** – Offsite backup settings must already be configured in the SonicWALL CDP Web Management Interface, and the offsite appliance must be available.
- **Do Not Send Files Offsite** – No files will be sent offsite.

Step 10 Select the desired schedule from the **Schedule** drop-down list.

Step 11 To activate this backup task, select the **Enable this task in Policy** checkbox. To disable this backup task without deleting it, you can clear this checkbox.

Step 12 Click **OK**.

Verifying SharePoint Backup Activity

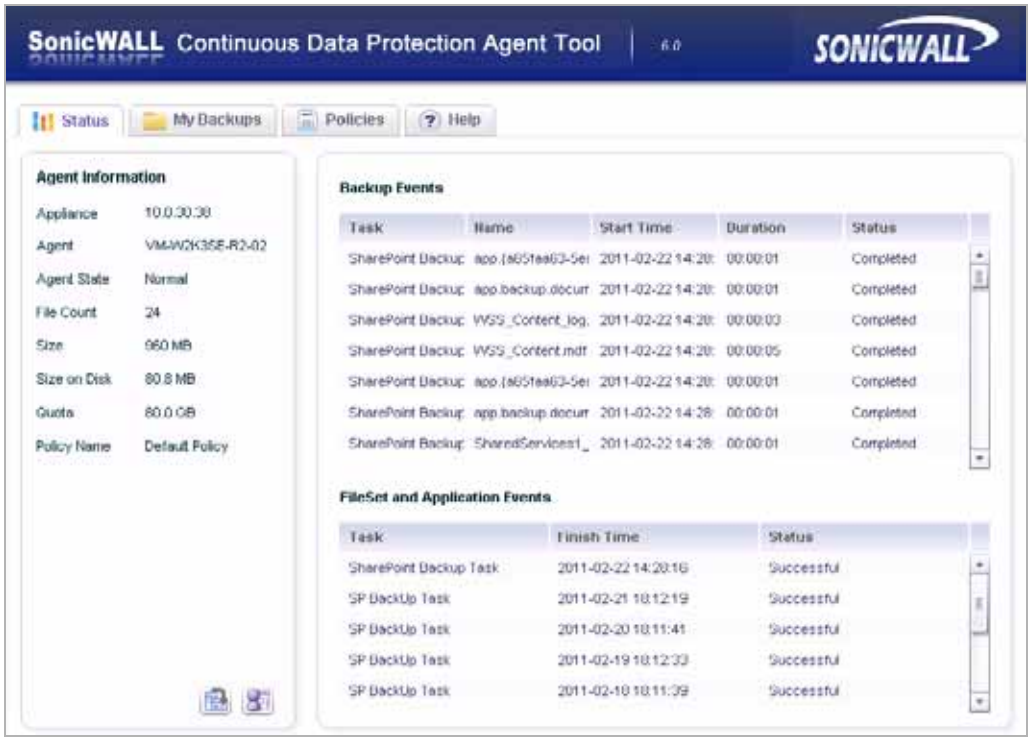
This section describes how to tell if your Microsoft SharePoint backups are working correctly. You can view log entries showing the backups in the **Status** page of the SonicWALL CDP Agent User Interface.

You should see log entries showing backups after each scheduled backup after creating a backup task for SharePoint.

Step 1 In the SonicWALL CDP Agent User Interface, click the **Status** tab.

Step 2 Optionally, to view backup status on a different appliance, click the change appliance button in the left pane.

Step 3 View the backup status in the right pane.


SonicWALL Continuous Data Protection Agent Tool
SONICWALL
Status
My Backups
Policies
Help
Agent Information
Appliance 10.0.30.30
Agent VMWIN2K3SE-R2-02
Agent State Normal
File Count 24
Size 960 MB
Size on Disk 80.8 MB
Quota 80.0 GB
Policy Name Default Policy
Backup Events
Task Name Start Time Duration Status
SharePoint Backup app.{a65fea63-5e 2011-02-22 14:20: 00:00:01 Completed
SharePoint Backup app.backup.docum 2011-02-22 14:20: 00:00:01 Completed
SharePoint Backup WSS_Content_log. 2011-02-22 14:20: 00:00:03 Completed
SharePoint Backup WSS_Content.mdf 2011-02-22 14:20: 00:00:05 Completed
SharePoint Backup app.{a65fea63-5e 2011-02-22 14:20: 00:00:01 Completed
SharePoint Backup app.backup.docum 2011-02-22 14:28: 00:00:01 Completed
SharePoint Backup SharedServices1_ 2011-02-22 14:28: 00:00:01 Completed
FileSet and Application Events
Task Finish Time Status
SharePoint Backup Task 2011-02-22 14:20:16 Successful
SP BackUp Task 2011-02-21 18:12:19 Successful
SP BackUp Task 2011-02-20 18:11:41 Successful
SP BackUp Task 2011-02-19 18:12:33 Successful
SP BackUp Task 2011-02-18 18:11:39 Successful

Step 4 Click the **My Backups** tab and view the list of backup revisions.

Backing up System State and Active Directory

Active Directory is included within the System State application object in SonicWALL CDP 6.0 and higher. When creating a System State application object, you can select components, including Active Directory, to back up. This allows you to backup and recover Active Directory revisions from agent machines together with interdependent system files to provide a consistent environment.

Note System State and Active Directory cannot be backed up from the Web Management Interface. Use the Agent User Interface to configure System State and Active Directory for backup.

See the following sections:

- "Creating an Application Object for System State and Active Directory" section on page 156
- "Scheduling Backups for System State and Active Directory" section on page 158
- "Configuring a Backup Task for System State" section on page 158
- "Verifying System State and Active Directory Backup Activity" section on page 159

Creating an Application Object for System State and Active Directory

To backup System State and Active Directory, you must configure an application object, a schedule, and a backup task that includes both the application object and the schedule. This section describes how to create the application object.

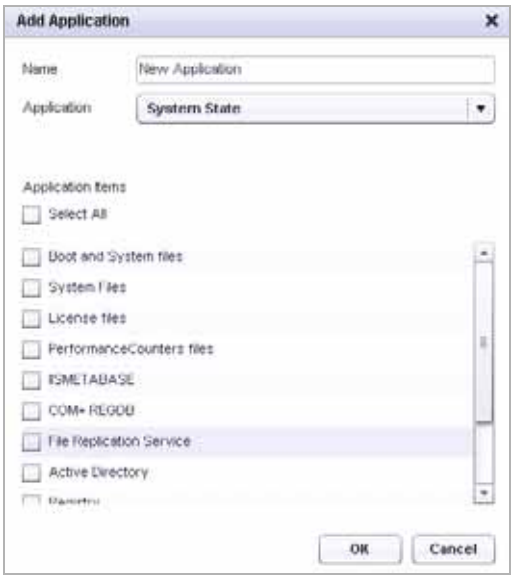
To backup System State and Active Directory using the Agent User Interface, perform the following steps:

Step 1 Open the **SonicWALL Agent User Interface** on the Domain Controller.

Step 2 In the SonicWALL CDP Agent User Interface, click the **Policies** tab.

Step 3 In the left pane, click **Applications**.

Step 4 In the right pane, click the Plus button at the lower right corner. The Add Application window opens.



Step 5 Type a descriptive name for the application object into the **Name** field.

Step 6 Select **System State** in the **Application** drop-down list. The list of available applications is automatically populated through a discovery process. For proper discovery, the Microsoft Volume Shadow Copy service must not be disabled. See "Backup and Recovery Troubleshooting" on page 229 for more information.

Step 7 Under **Application items**, select the checkboxes for one or more System State components to back up. You can select **Active Directory** in this screen. SonicWALL recommends selecting the **Select All** checkbox to ensure that all associated System State files are backed up along with Active Directory.

The exact list of system components that make up your computer's System State data depend on the computer's operating system and configuration. For example, on a Windows Server you might see the following:

- Boot and System files
- System files
- License files
- PerformanceCounters files
- IISMETASBASE
- COM+REGDB
- File Replication Service
- Active Directory
- Registry
- Windows Management Instrumentation
- Event Logs

Step 8 In the Add Application window, click **OK** to add the application object.

The new application object appears in the **Policies** screen of the Agent User Interface.

Note Before the backup will occur, you must also configure a schedule for this application object, and a backup task that includes both the application object and the schedule.

Scheduling Backups for System State and Active Directory

A schedule is required when creating an Application backup task to backup System State and Active Directory. You can use the same schedule object in more than one backup task.

For instructions on creating a schedule object, see the "Creating Schedules for Application Backups" section on page 124.

Configuring a Backup Task for System State

A backup task includes both an application object and a schedule for the backup. Without a backup task, no backups will occur.

For offsite backup, you can choose the **Send All Files Offsite** option when adding or editing a backup task.

Note Before creating a backup task, create the application object and schedule to be included in the task.

To create a backup task for a System State and Active Directory backup, perform the following steps:

Step 1 In the SonicWALL CDP Agent User Interface, click the **Policies** tab.

Step 2 In the left pane, select **Backup Tasks**.

Step 3 In the right pane, click the Plus button at the lower right corner. The Add Backup Task window opens.

Step 4 Type a descriptive name for the backup task into the **Name** field.

Step 5 Select **Application** from the **Select File Type** drop-down list.

Step 6 Select the desired application object from the **Application Data** drop-down list.

Step 7 Type the desired number of backup revisions to keep into the **Number of Versions** field. The default is 2.

Step 8 The **Trimming Algorithm** field is not configurable for Application policies. The field displays the type of trimming algorithm in use.

Step 9 In the **Offsite** drop-down list, select one of the following options:

- **Send all Files Offsite** – Offsite backup settings must already be configured in the SonicWALL CDP Web Management Interface, and the offsite appliance must be available.
- **Do Not Send Files Offsite** – No files will be sent offsite.

Step 10 Select the desired schedule from the **Schedule** drop-down list.

Step 11 To activate this backup task, select the **Enable this task in Policy** checkbox. To disable this backup task without deleting it, you can clear this checkbox.

Step 12 Click **OK**.

Verifying System State and Active Directory Backup Activity

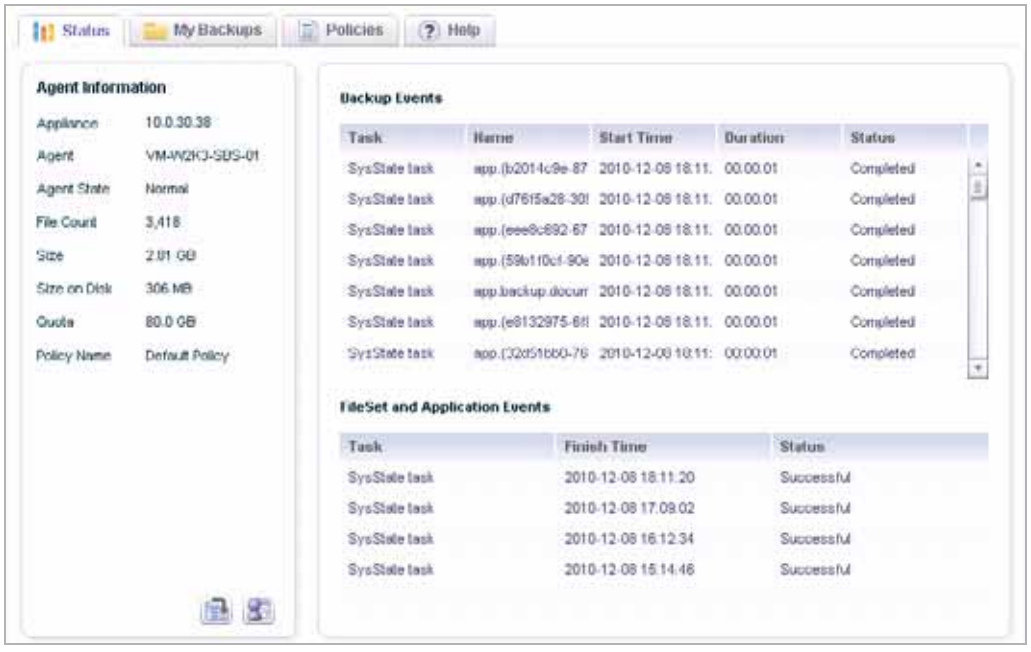
This section describes how to tell if your System State backups are working correctly. You can view log entries showing the backups in the **Status** page of the SonicWALL CDP Agent User Interface.

You should see log entries showing backups after each scheduled backup after creating a backup task for System State and Active Directory.

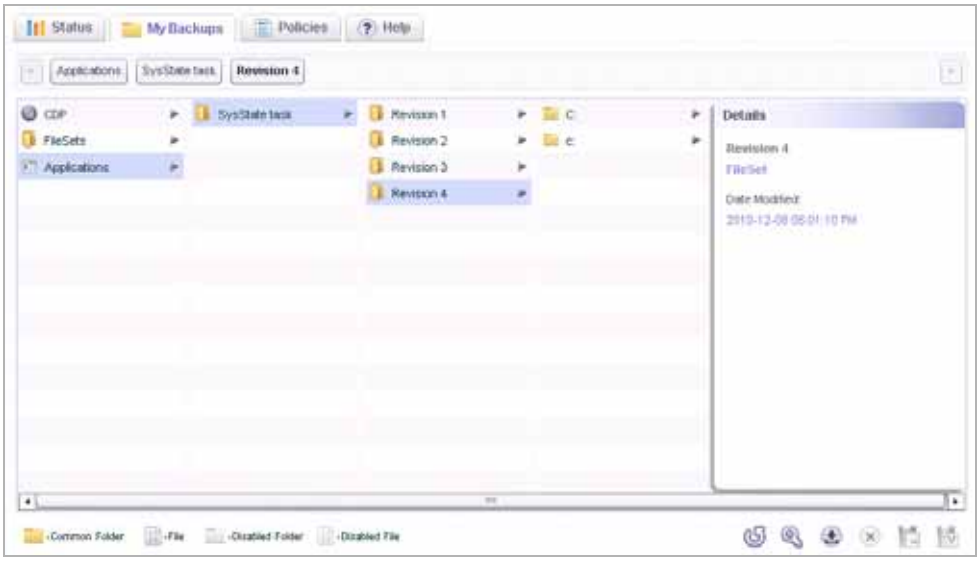
Step 1 In the SonicWALL CDP Agent User Interface, click the **Status** tab.

Step 2 Optionally, to view backup status on a different appliance, click the change appliance button in the left pane.

Step 3 View the backup status in the right pane.



Step 4 Click the **My Backups** tab and view the list of backup revisions.

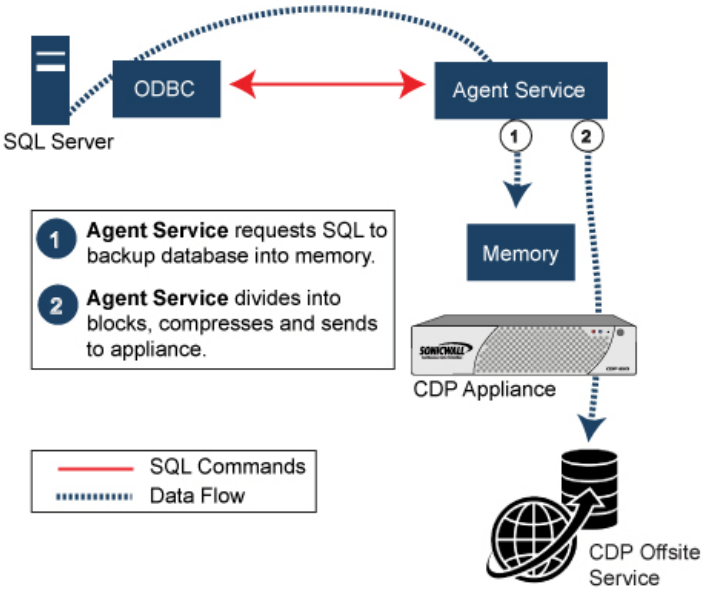


Backing up Microsoft SQL Server

Backing up Microsoft SQL Server using SonicWALL CDP allows users to store and retrieve Microsoft SQL Server revisions from an agent machine. Microsoft SQL databases are configured for backup using the SonicWALL CDP Agent User Interface.

Note Microsoft SQL Server backup can only be configured using the Agent User Interface.

During SQL backup and restore using CDP, the Agent Service directly interfaces with the Microsoft SQL server through the Open Database Connectivity (ODBC) API, using an SQL-ODBC driver that is installed with SQL. By ODBC, the Agent service communicates to the SQL server through transactional SQL commands.



When the SonicWALL CDP Agent Service backs up an SQL database, it instructs SQL to place the data in a certain location in memory. The Agent Service will then process the data one block at a time, compressing it and sending to the appliance.

The Agent Service first needs to connect to the database and authenticate using either Windows user account credentials or using an SQL account. More details are provided in the "SQL Authentication" section on page 167.

This section contains the following subsections:

- "Adding a SQL Server Backup Application Object" section on page 162
- "Scheduling Backups for Microsoft SQL" section on page 163
- "Configuring a Backup Task for Microsoft SQL Database Backups" section on page 163
- "Verifying SQL Account Configuration" section on page 166
- "SQL Authentication" section on page 167

Adding a SQL Server Backup Application Object

To backup Microsoft SQL databases, you must configure an application object, a schedule, and a backup task that includes both the application object and the schedule. This section describes how to create the application object.

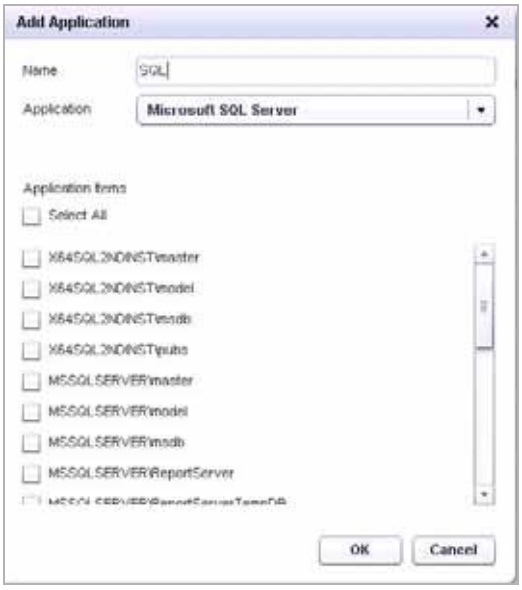
To create an application object for Microsoft SQL database backup, perform the following steps:

Step 1 Open the **SonicWALL Agent User Interface** on the SQL server.

Step 2 In the SonicWALL CDP Agent User Interface, click the **Policies** tab.

Step 3 In the left pane, click **Applications**.

Step 4 In the right pane, click the Plus button at the lower right corner. The Add Application window opens.



Step 5 Type a descriptive name for the application object into the **Name** field.

Step 6 Select either **Microsoft SQL Server** or **Microsoft SQL Server Desktop Engine (MSDE)** in the **Application** drop-down list. The list of available applications is automatically populated through a discovery process. For proper discovery, the Microsoft Volume Shadow Copy and VSS Writer services must not be disabled. See "Backup and Recovery Troubleshooting" on page 229 for more information.

Step 7 Under **Application items**, select the checkboxes for one or more databases to back up.

Step 8 In the Add Application window, click **OK** to add the application object.

The new application object appears in the **Policies** screen of the Agent User Interface.

Note Before the backup will occur, you must also configure a schedule for this application object, and a backup task that includes both the application object and the schedule.

Scheduling Backups for Microsoft SQL

A schedule is required when creating an Application backup task to backup Microsoft SQL databases. You can use the same schedule object in more than one backup task.

For instructions on creating a schedule object, see the "Creating Schedules for Application Backups" section on page 124.

Configuring a Backup Task for Microsoft SQL Database Backups

A backup task includes both an application object and a schedule for the backup. Without a backup task, no backups will occur.

For offsite backup, you can choose the **Send All Files Offsite** option when adding or editing a backup task.

Note Before creating a backup task, create the application object and schedule to be included in the task.

To create a backup task for Microsoft SQL database backup, perform the following steps:

Step 1 In the SonicWALL CDP Agent User Interface, click the **Policies** tab.

Step 2 In the left pane, select **Backup Tasks**.

Step 3 In the right pane, click the Plus button at the lower right corner. The Add Backup Task window opens.

Step 4 Type a descriptive name for the backup task into the **Name** field.

Step 5 Select **Application** from the **Select File Type** drop-down list.

Step 6 Select the desired application object from the **Application Data** drop-down list.

Step 7 Type the desired number of backup revisions to keep into the **Number of Versions** field. The default is 2.

Step 8 The **Trimming Algorithm** field is not configurable for Application policies. The field displays the type of trimming algorithm in use.

Step 9 In the **Offsite** drop-down list, select one of the following options:

- **Send all Files Offsite** – Offsite backup settings must already be configured in the SonicWALL CDP Web Management Interface, and the offsite appliance must be available.
- **Do Not Send Files Offsite** – No files will be sent offsite.

Step 10 Select the desired schedule from the **Schedule** drop-down list.

Step 11 To activate this backup task, select the **Enable this task in Policy** checkbox. To disable this backup task without deleting it, you can clear this checkbox.

Step 12 Click **OK**.

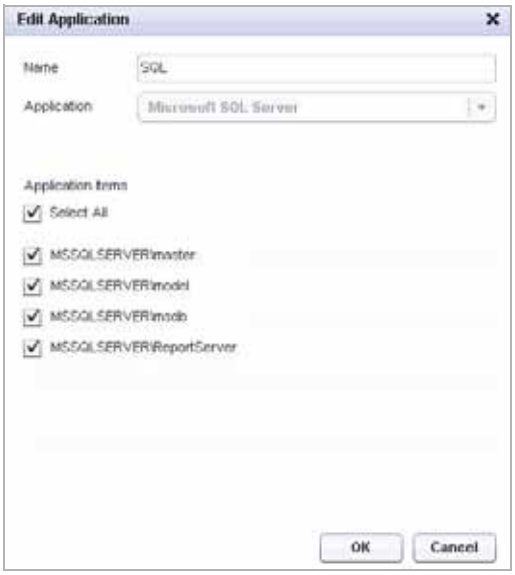
Removing a SQL Database from the Backup Task

To remove a database from the list of SQL databases scheduled for backup, perform the following steps:

Step 1 In the SonicWALL CDP Agent User Interface, click the **Policies** tab.

Step 2 In the left pane, select **Applications**.

Step 3 In the right pane, click the Edit button for the application object you wish to edit. The Edit Application window opens.



Step 4 Clear the checkbox for the database you wish to delete.

Step 5 Click **OK**.

Verifying Microsoft SQL Backup Activity

This section describes how to tell if your Microsoft SQL backups are working correctly. You can view log entries showing the backups on the **Status** page of the SonicWALL CDP Agent User Interface.

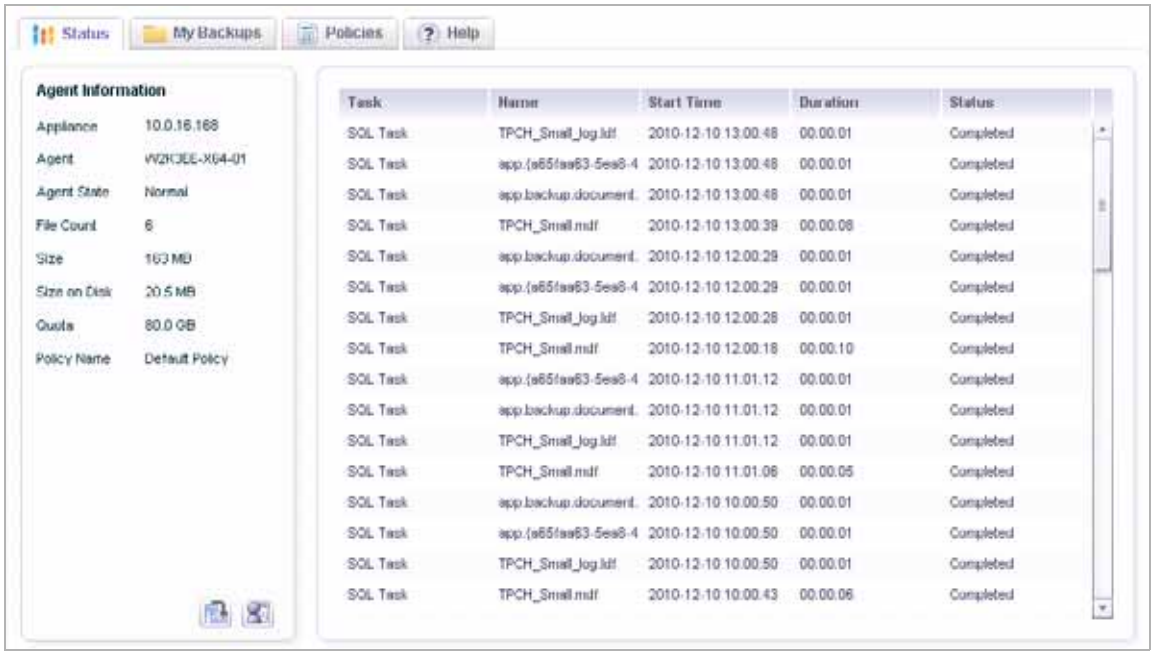
You should see log entries showing backups after each scheduled backup after creating a backup task for SQL.

To view the status of SQL backups:

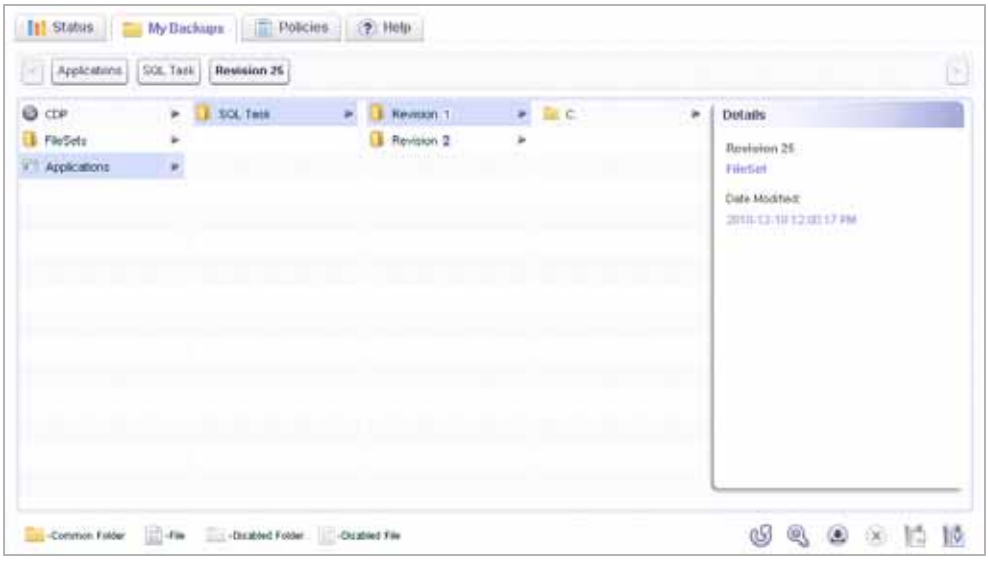
Step 1 In the SonicWALL CDP Agent User Interface, click the **Status** tab.

Step 2 Optionally, to view backup status on a different appliance, click the change appliance button in the left pane.

Step 3 View the backup status in the right pane.


Status
My Backups
Policies
Help
Agent Information
Appliance 10.0.16.168
Agent W2K3EE-X64-01
Agent State Normal
File Count 6
Size 163 MB
Size on Disk 20.5 MB
Quota 80.0 GB
Policy Name Default Policy
Task
Name
Start Time
Duration
Status
SQL Task TPCH_Small_log.ldf 2010-12-10 13:00:48 00.00.01 Completed
SQL Task app.{a65faa63-5ea8-4 2010-12-10 13:00:48 00.00.01 Completed
SQL Task app.backup.document 2010-12-10 13:00:48 00.00.01 Completed
SQL Task TPCH_Small.mdf 2010-12-10 13:00:39 00.00.08 Completed
SQL Task app.backup.document 2010-12-10 12:00:29 00.00.01 Completed
SQL Task app.{a65faa63-5ea8-4 2010-12-10 12:00:29 00.00.01 Completed
SQL Task TPCH_Small_log.ldf 2010-12-10 12:00:28 00.00.01 Completed
SQL Task TPCH_Small.mdf 2010-12-10 12:00:18 00.00.10 Completed
SQL Task app.{a65faa63-5ea8-4 2010-12-10 11:01:12 00.00.01 Completed
SQL Task app.backup.document 2010-12-10 11:01:12 00.00.01 Completed
SQL Task TPCH_Small_log.ldf 2010-12-10 11:01:12 00.00.01 Completed
SQL Task TPCH_Small.mdf 2010-12-10 11:01:06 00.00.05 Completed
SQL Task app.backup.document 2010-12-10 10:00:50 00.00.01 Completed
SQL Task app.{a65faa63-5ea8-4 2010-12-10 10:00:50 00.00.01 Completed
SQL Task TPCH_Small_log.ldf 2010-12-10 10:00:50 00.00.01 Completed
SQL Task TPCH_Small.mdf 2010-12-10 10:00:43 00.00.06 Completed

Step 4 Click the **My Backups** tab and view the list of backup revisions.



SQL Configuration Levels

SQL backup configuration is set at different levels. These are:

- Agent (or application) Level: Offsite backup is set on the entire agent.
- SQL Instance Level: More than one SQL instance can be running on a same machine.
- Database Level: An instance can contain one or more databases. The databases are backed up independently.

Servers normally have only one instance, which matches the Windows computer name. SQL instances can be created to allow for completely separate database management access to different databases.

Also, an instance will be created for each database version installed on the same machine. For example, SQL 2000 and SQL 2005 can run on the same server, but they will have different instances.

For example, Offsite Backup is applied to the entire agent, meaning that all selected instances and databases will be backed up to offsite. Authentication is set at an instance level.

Offsite Backup of SQL

Offsite Service backup of CDP is set at the agent level when configuring the backup task. This implies that all SQL instances and databases selected on the agent will be backed up to the Offsite Service.

You can view files backed up offsite by expanding the **Offsite** option while logged into the Agent as Administrator. For information about this, see the “Using the Agent UI as Administrator” section on page 96.

SQL Database Maintenance

Databases can become corrupted over time. Therefore, it is common practice to run a Database Consistency Check (DBCC) periodically to make sure that the database is healthy.

Verifying SQL Account Configuration

In order to backup a database, the SQL account used to access the SQL database must have:

- System administrators role
- Database Owner Role (db_owner)
- Access Rights to Database to back up

In general, a user called “sa” is created when SQL is installed.

To verify the SQL account configuration, perform the following steps:

Step 1 In the SQL management Interface, highlight the SQL account on the right hand side of the screen and double click it.

Step 2 Expand the security tab under the SQL server instance.

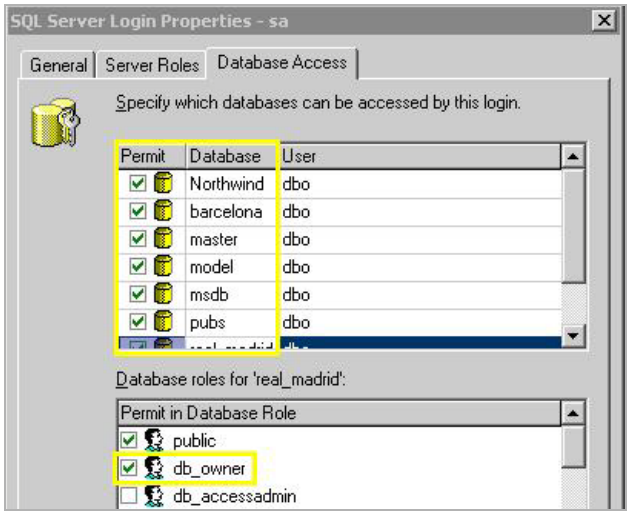
Step 3 Click **Logins**.

Step 4 Click the **Server Roles** tab.

Step 5 Select the **System Administrators** role.

Step 6 Click the **Database Access** tab.

Step 7 Make sure that the user has the **db_owner** role, and make sure that access is permitted to the databases to backup.



SQL Authentication

For access to Microsoft SQL Server, SonicWALL CDP uses Windows Authentication in which the Windows user credentials are submitted to SQL.

This section contains the following subsections:

- "Authentication Modes in Microsoft SQL Server" section on page 167
- "About Windows Authentication" section on page 168
- "About SQL Server Authentication" section on page 169
- "Setting Up Windows Authentication Mode Security" section on page 169
- "Setting Up Mixed Mode Security" section on page 170

Authentication Modes in Microsoft SQL Server

Microsoft SQL Server can operate in one of two security (authentication) modes:

- Windows Authentication Mode (Windows Authentication)
- Mixed Mode (Windows Authentication and SQL Server Authentication)

Windows Authentication mode allows a user to connect through a Microsoft Windows user account.

Mixed Mode allows users to connect to an instance of SQL Server using either Windows Authentication or SQL Server Authentication. Users who connect through a Windows user account can make use of trusted connections in either Windows Authentication Mode or Mixed Mode.

SQL Server Authentication is provided for backward compatibility. For example, if you create a single Windows 2000 group and add all necessary users to that group, you will need to grant the Windows 2000 group login rights to SQL Server and access to any necessary databases.

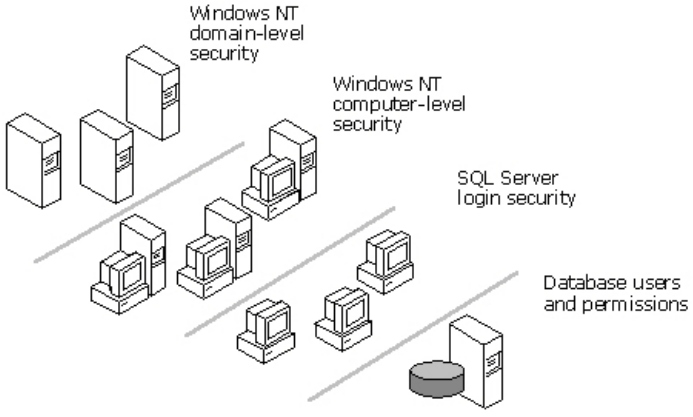
About Windows Authentication

When a user connects through a Windows user account, SQL Server revalidates the account name and password by calling back to Windows for the information.

SQL Server achieves login security integration with Windows by using the security attributes of a network user to control login access. A user's network security attributes are established at network login time and are validated by a Windows domain controller. When a network user tries to connect, SQL Server uses Windows-based facilities to determine the validated network user name. SQL Server then verifies that the person is who they say they are, and then permits or denies login access based on that network user name alone, without requiring a separate login name and password.

Login security integration operates over any supported network protocol in SQL Server.

Note that if a user attempts to connect to an instance of SQL Server providing a blank login name, SQL Server uses Windows Authentication. Additionally, if a user attempts to connect to an instance of SQL Server configured for Windows Authentication Mode by using a specific login, the login is ignored and Windows Authentication is used.



Windows Authentication has certain benefits over SQL Server Authentication, primarily due to its integration with Windows security system. Windows security provides more features, such as secure validation and encryption of passwords, auditing, password expiration, minimum password length, and account lockout after multiple invalid login requests.

Because Windows users and groups are maintained only by Windows, SQL Server reads information about a user's membership in groups when the user connects. If changes are made to the accessibility rights of a connected user, the changes become effective the next time the user connects to an instance of SQL Server or logs on to Windows (depending on the type of change).

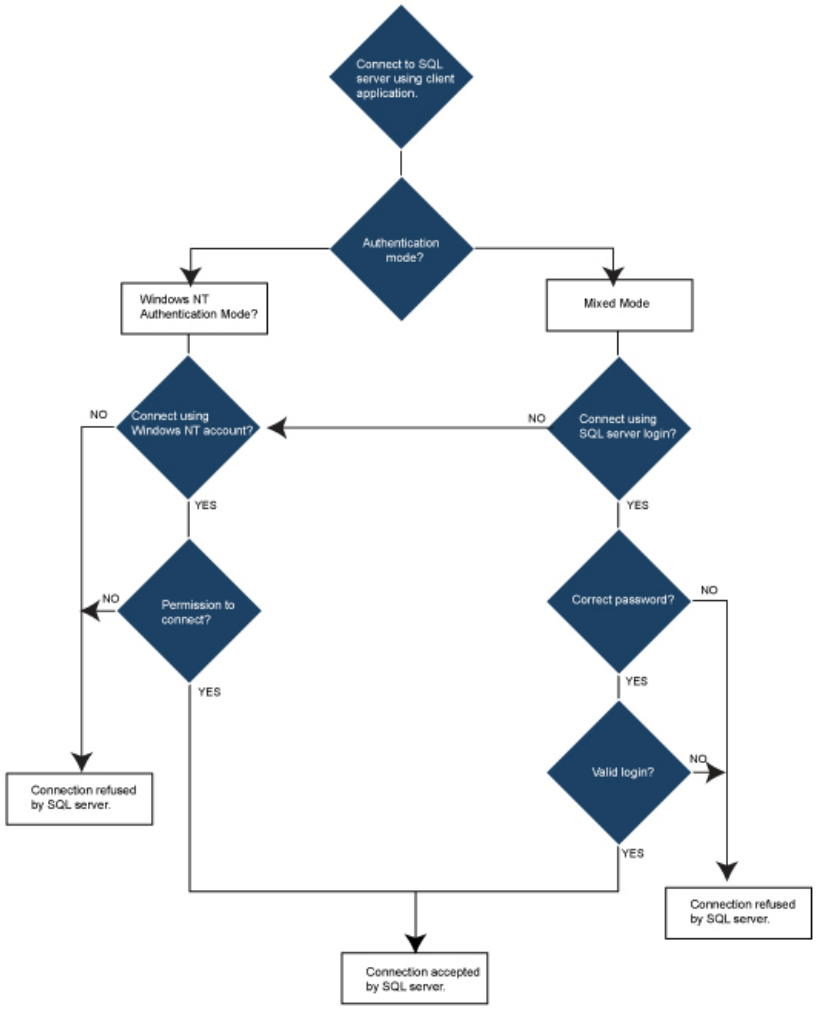
About SQL Server Authentication

When a user connects with a specified login name and password from a non-trusted connection, SQL Server performs the authentication itself by checking to see if a SQL Server login account has been set up and if the specified password matches the one previously recorded. If SQL Server does not have a login account set, authentication fails and the user receives an error message.

SQL Server Authentication is provided for backward compatibility because applications written for SQL Server version 7.0 or earlier may require the use of SQL Server logins and passwords.

Also, SQL Server Authentication may be required for connections with clients other than Windows clients.

Figure 1 SQL Server Security Decision Tree



Setting Up Windows Authentication Mode Security

To set up Windows Authentication Mode security with the SQL management interface:

Step 1 Expand a server group.

Step 2 Right-click a server, and then click **Properties**.

Step 3 On the **Security** tab, under **Authentication**, click **Windows only**.

Step 4 Under **Audit level**, select the level at which user accesses to Microsoft SQL Server are recorded in the SQL Server error log:

- **None** causes no auditing to be performed.
- **Success** causes only successful login attempts to be audited.
- **Failure** causes only failed login attempts to be audited.
- **All** causes successful and failed login attempts to be audited.

Setting Up Mixed Mode Security

To set up Mixed Mode security with the SQL management interface:

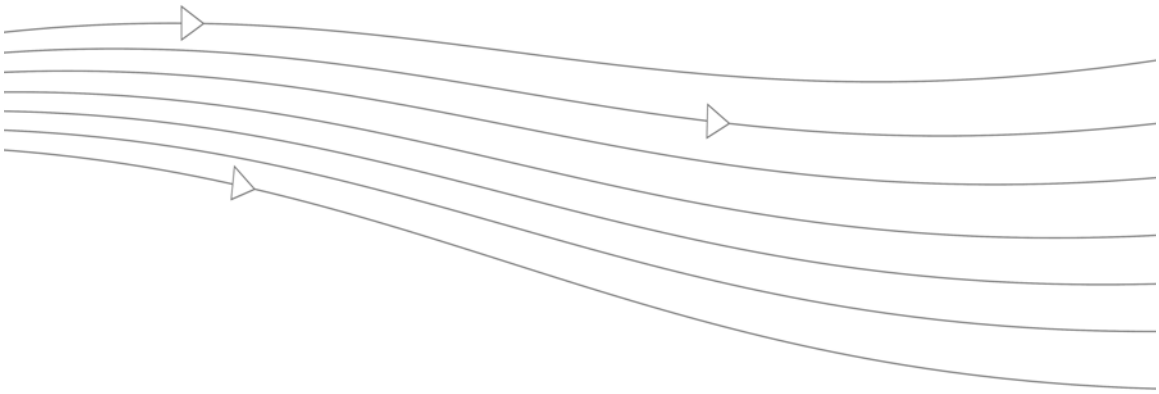
Step 1 Expand a server group.

Step 2 Right-click a server, and then click **Properties**.

Step 3 On the **Security** tab, under **Authentication**, click **SQL Server and Windows**.

Step 4 Under **Audit level**, select the level at which user accesses to Microsoft SQL Server are recorded in the SQL Server error log:

- **None** causes no auditing to be performed.
- **Success** causes only successful login attempts to be audited.
- **Failure** causes only failed login attempts to be audited.
- **All** causes successful and failed login attempts to be audited.



Chapter 11: Recovering Backed Up Data

When using SonicWALL CDP, if an agent should experience an event that results in data loss, you will be able to recover any data that you had defined for backup. This chapter provides information about recovering data directly from the SonicWALL CDP appliance.

This chapter provides procedures for recovering files, folders, and applications from SonicWALL CDP backups. See the following sections:

- "Recovering Files and Folders" section on page 172
- "Recovering Data from an Offsite Appliance" section on page 174
- "Recovering Data from Microsoft Exchange" section on page 176
- "Recovering SharePoint" section on page 189
- "Recovering System State and Active Directory" section on page 191
- "Recovering Data from Microsoft SQL Server" section on page 196

Recovering Files and Folders

SonicWALL CDP allows you to recover lost data directly from the appliance. Recovery can be performed to replace a file set that has been deleted, or to restore a previous version of a file or folder that has been changed or otherwise damaged. Recovery can be performed on any agent and recovered files are restored directly from the appliance. Files can also be recovered directly from an offsite, upstream appliance by the administrator.

If necessary, before restoring a file set, first follow the prescribed restore procedures of the system which may include the re-installation of the operating system, applications or replacement of hardware.

To recover files and folders from the SonicWALL CDP appliance, perform the following steps:

Step 1 Launch the **SonicWALL CDP Agent** software on the agent machine on which you want to recover the file set.

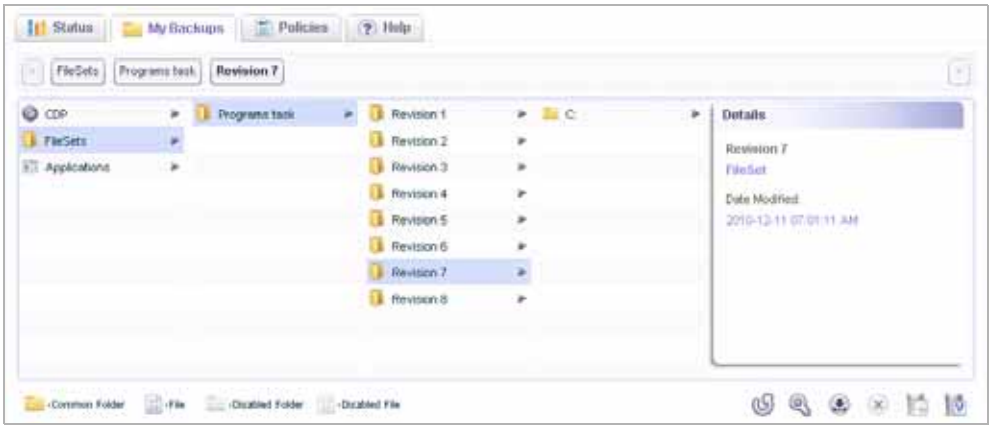
Step 2 If necessary, click the Change Appliance icon to change the SonicWALL CDP appliance to the one with the files you need.

Step 3 Click the **My Backups** tab.

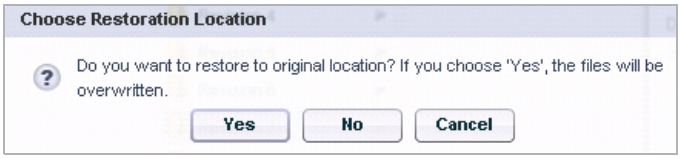
Step 4 In the left pane, click **FileSets**. The display expands to show available backup tasks.

Step 5 Click the desired backup task. The available revisions are displayed.

Step 6 Click the desired revision. The root folder and details about the revision are displayed, including the date and time.

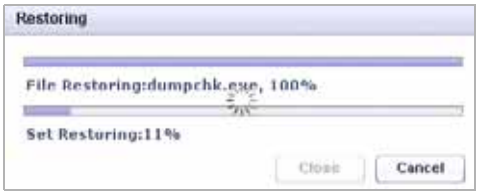


Step 7 At the bottom right corner, click the Restore icon . The Choose Restoration Location dialog opens.

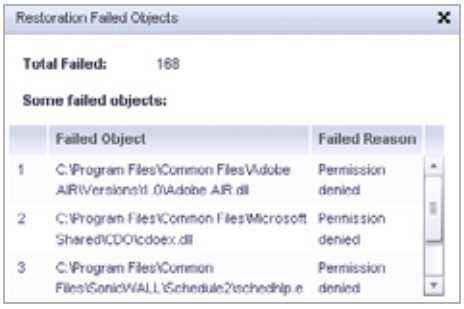

Choose Restoration Location
Do you want to restore to original location? If you choose 'Yes', the files will be overwritten.
Yes
No
Cancel

Click **Yes** to restore the files on top of the original files. Click **No** to save the files to another location on disk. Click **Cancel** to exit the restoration process without restoring the files at all.

The Restoring window displays the progress of the restore.



Step 8 If any files cannot be restored, the Restoration Failed Objects window displays a list of files and the reasons for their failure to restore. Click the **X** to close the window.


Restoration Failed Objects
Total Failed: 168
Some failed objects:
Failed Object
Failed Reason
1 C:\Program Files\Common Files\Adobe AIR\Versions\1.0\Adobe AIR.dll Permission denied
2 C:\Program Files\Common Files\Microsoft Shared\CDO\cdoex.dll Permission denied
3 C:\Program Files\Common Files\SonicWALL\Schedule2\schedhlp.e Permission denied

Step 9 When the restore process is finished, the Restoring window changes to Done. Click the **Close** button to close the window.

Recovering Data from an Offsite Appliance

The administrator can recover data directly from an offsite appliance when logged in to the Administrative File Browser in the SonicWALL CDP Agent User Interface.

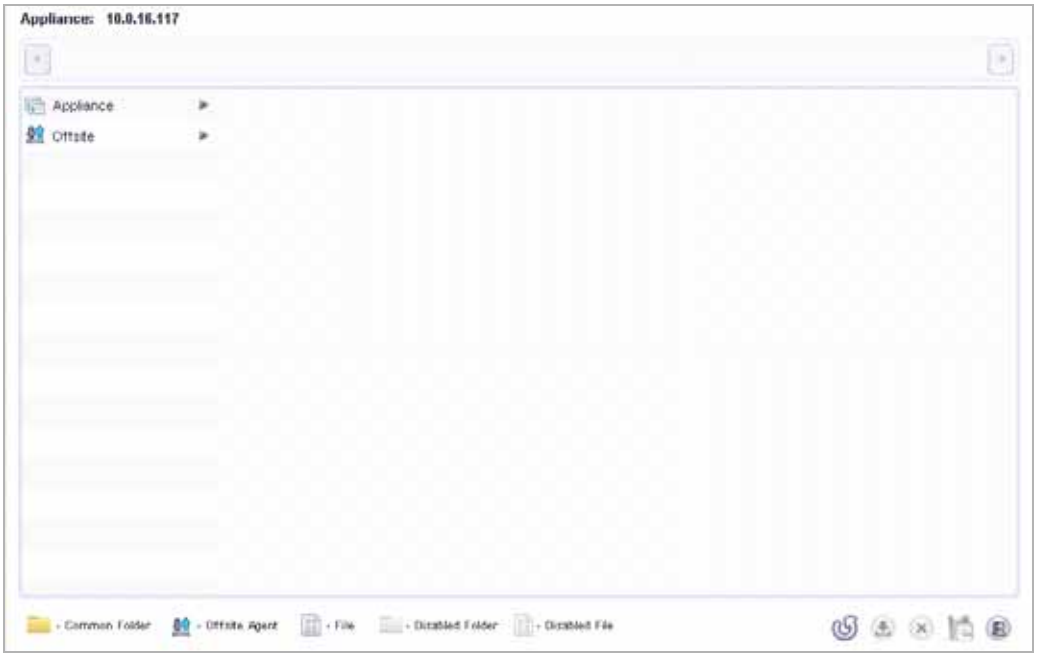
To restore data from an offsite, upstream appliance, perform the following steps:

Step 1 Launch the SonicWALL CDP Agent User Interface on the agent to which you want to restore the data.

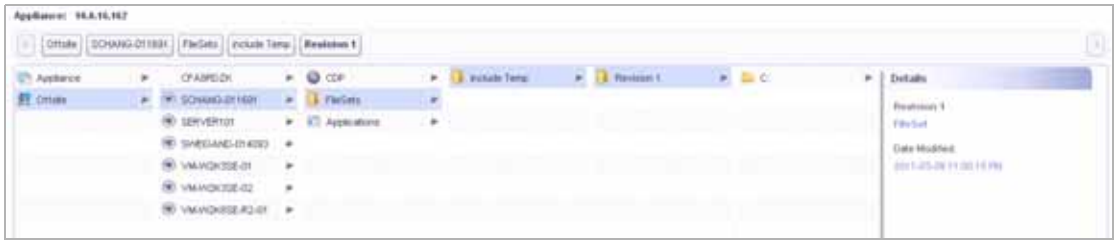
Step 2 On the Status tab, click the **Login to Administrator File Browser** button.

Step 3 In the login dialog box, type in the IP address of the SonicWALL CDP appliance to which you want to connect.

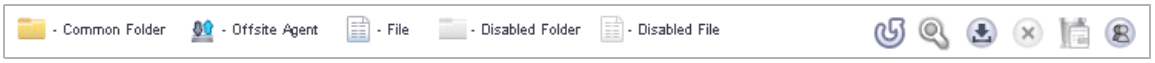
Step 4 Type in the password for the admin account, and click **Login**. The Agent User Interface displays the starting screen for the appliance.



Step 5 Click the arrow for **Offsite** to expand the display to include all associated agents, then click any agent to expand the display further and view specific backups.



The bottom of the window provides controls for your use.

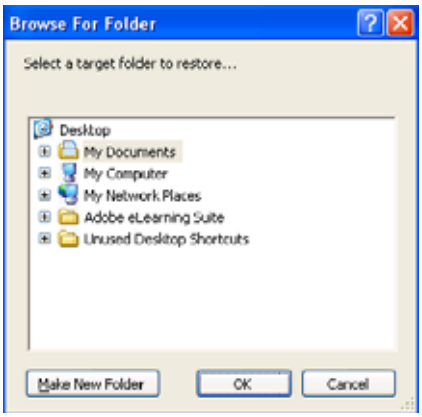


At the right, the following controls are available, from left to right:

- Refresh – refreshes the window contents
- Search – search for an item
- Restore – restores the selected item
- Remove Items – removes the selected items
- Remove Deleted Items – removes items that are no longer on the agent machine
- Logoff from Administrator File Browser – logs off

Step 6 Click the **Restore** button.

Step 7 In the Browse For Folder window, either expand the displayed folders and select the folder in which to place the restored file, or click the **Make New Folder** button and create a new folder for it. Click **OK**.



The data is downloaded to your folder.

Recovering Data from Microsoft Exchange

Recovery of data from Microsoft Exchange using SonicWALL CDP allows users to retrieve Microsoft Exchange revisions from an agent machine previously configured to backup that data.

Note Microsoft Exchange data can be restored using the Web Management Interface or Agent User Interface. Exchange restore using Web Management Interface can restore to disk any Exchange database, even for servers on different agents than the Web Management Interface.

See the following sections:

- "Recovering Exchange 2010 User Mailboxes" section on page 176
- "Recovering Exchange 2010 InfoStore" section on page 179
- "Recovering an Exchange 2007/2003 User Mailbox" section on page 181
- "Recovering an Exchange 2007/2003 Storage Group" section on page 184

Recovering Exchange 2010 User Mailboxes

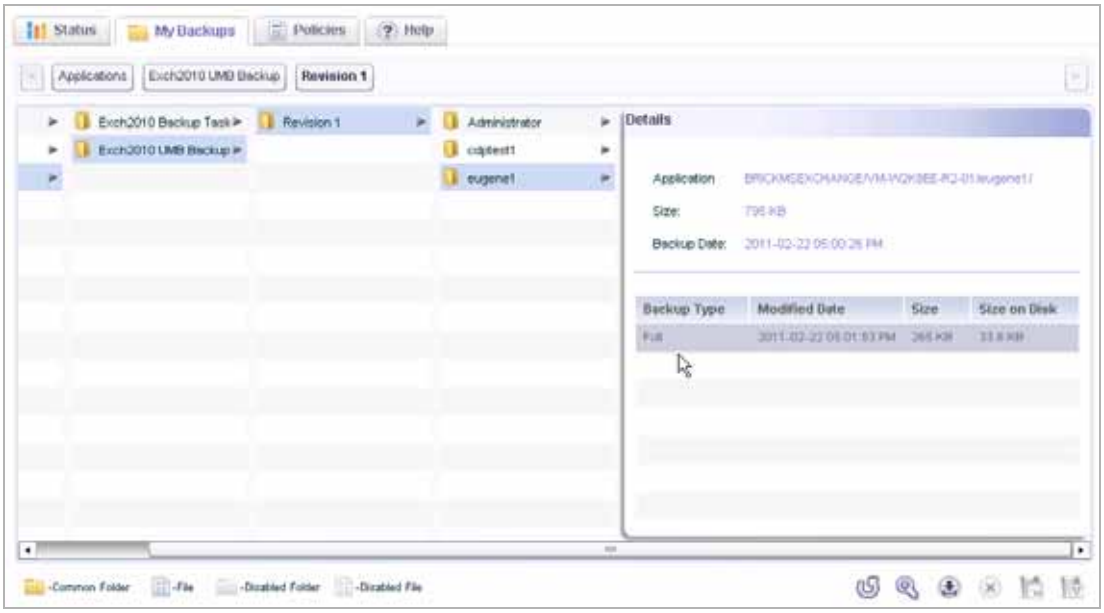
This section describes how to restore an individual user mailbox backup to the Exchange 2010 server, by using the Microsoft Exchange User Mailbox Backup and Restore server application in the SonicWALL CDP Agent User Interface.

Note You must log into the agent machine as **Administrator** before restoring a User Mailbox. For information about configuring the Administrator account for Exchange authentication, see "Configuring Authentication on the Exchange Server" on page 130. For more information about account privileges to access the Exchange server, see KB821897.

A mailbox must exist in Exchange in order for the restore to work properly. To restore an individual user mailbox to the Exchange server, perform the following steps:

Step 1 In the SonicWALL CDP Agent User Interface, click the **My Backups** tab.

Step 2 In the left pane, click **Applications**. The display expands to show available backup tasks.



Step 3 Click the desired backup task. The available revisions are displayed.

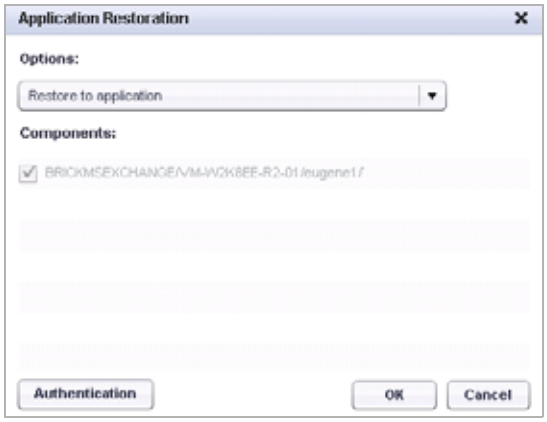
Step 4 Click the desired revision. The root folder and details about the revision are displayed, including the date and time.

Note To restore all user mailboxes contained in the revision, click the Restore icon and skip the next two steps.

Step 5 To restore a single user mailbox, click the desired user mailbox to restore. The Details are displayed.

Step 6 In the **Details** section, click to select the desired backup in the table in the lower area of the Details section, such as the **Full** backup of the mailbox.

Step 7 At the bottom right corner, click the Restore icon . The Application Restoration window opens.



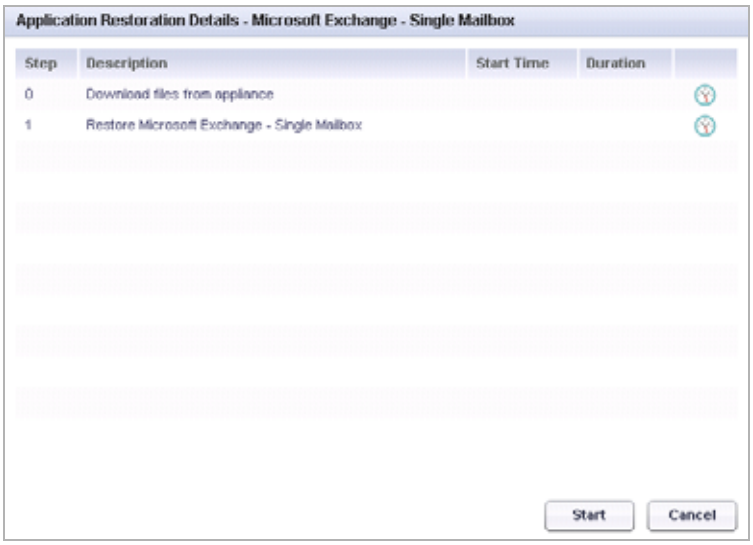
Step 8 For a *single user mailbox restoration*, select Restore to application from the **Options** drop-down list. No other option is available in this case.

When *restoring all mailboxes in a Revision*, select one of the following from the **Options** drop-down list:

- **Restore to original location** – This option restores the files to the Microsoft Exchange application location.
- **Restore to alternate location** – This option restores the files to the disk of the agent machine.

Step 9 Under **Components**, select the checkboxes for the user mailbox databases you want to restore. Select all databases to maintain consistency.

Step 10 Click **OK**. The Application Restoration Details window appears.

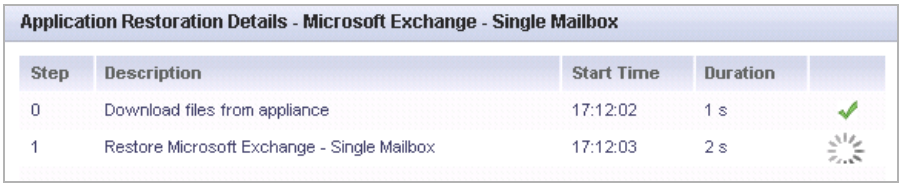


Step 11 The restoration steps are listed, along with a **Start Time** column, a **Duration** column, and an in-progress indicator. The steps are:

- **Download files from appliance**
- **Restore Microsoft Exchange - Single Mailbox**

To start the restore process, click **Start**. To exit without restoring any files, click **Cancel**.

The in-progress indicators become active for each step as it is executed, and the **Start Time** and **Duration** values are updated.



Step 12 When the restore is finished, click **Close**.

Note After the data is restored to the Exchange server, you may need to synchronize your local mail client (Outlook) in order to see restored emails.

Recovering Exchange 2010 InfoStore

You can restore Exchange 2010 InfoStore databases by using the SonicWALL CDP Microsoft Exchange InfoStore Backup and Restore server application in the SonicWALL CDP Agent User Interface.

This section describes how to restore an individual Storage Group. You can restore the Storage Group in two ways:

- Restore to Application - Copies the data directly to the Exchange database
- Restore to Disk - Copies the data to a folder on the local disk, then you can copy it to the Exchange database

A storage group must exist in Exchange in order for the restore to work properly.

Note The current account must have privileges to access the Exchange server. If authentication is configured for the Administrator account, login as Administrator to do the restore. For information about configuring the Administrator account for Exchange authentication, see "Configuring Authentication on the Exchange Server" on page 130. See also KB867704 and KB824126.

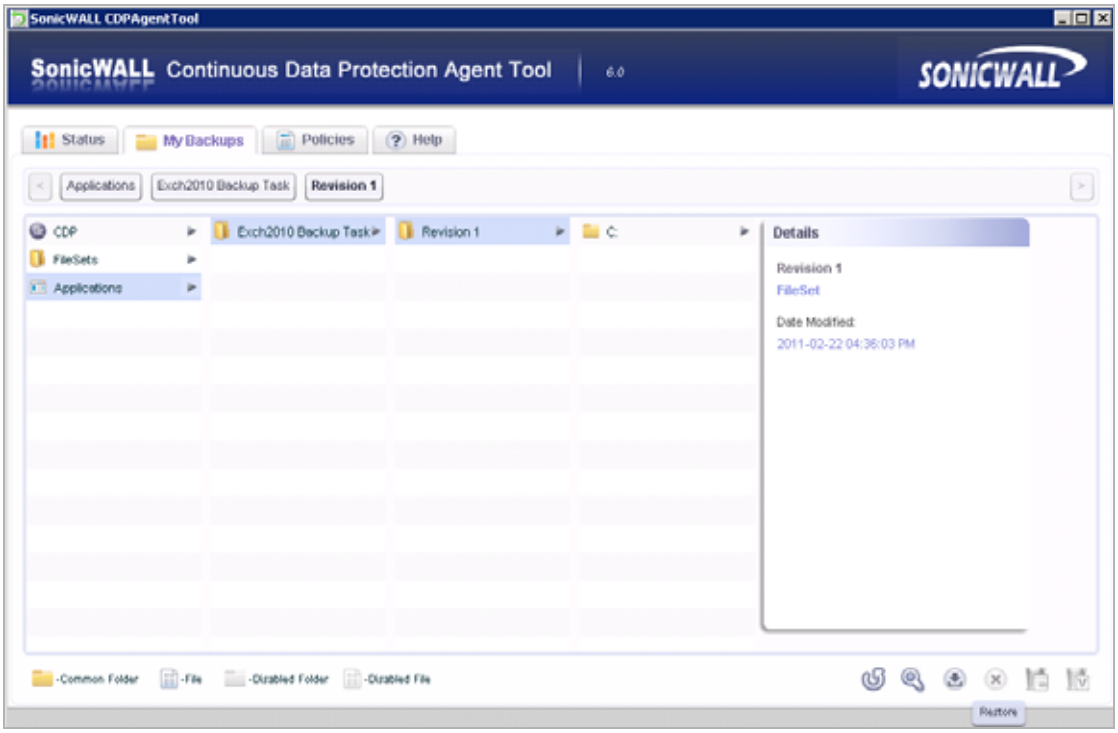
To restore InfoStore data using the SonicWALL CDP Agent User Interface, perform the following steps:

Step 1 In the SonicWALL CDP Agent User Interface, click the **My Backups** tab.

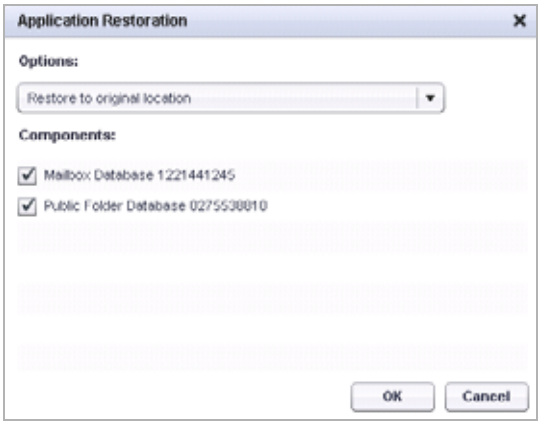
Step 2 In the left pane, click **Applications**. The display expands to show available backup tasks.

Step 3 Click the desired backup task. The available revisions are displayed.

Step 4 Click the desired revision. The root folder and details about the revision are displayed, including the date and time.



Step 5 At the bottom right corner, click the Restore icon . The Application Restoration window opens.

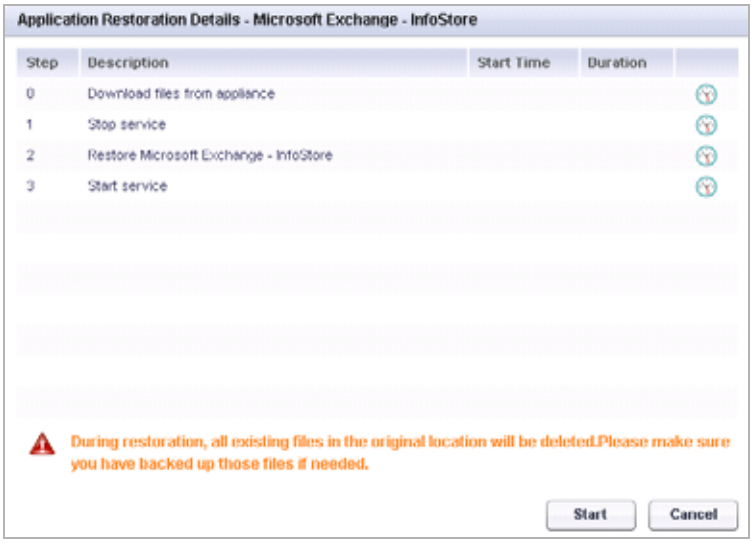


Step 6 In the **Options** drop-down list, select one of the following:

- **Restore to original location** – This option restores the files to the application in their original location in Microsoft Exchange.
- **Restore to alternate location** – This option restores the files to the disk of the agent machine.

Step 7 Under **Components**, select the checkboxes for the databases you want to restore.

Step 8 Click **OK**. The Application Restoration Details window appears.


Application Restoration Details - Microsoft Exchange - InfoStore
Step
Description
Start Time
Duration
0 Download files from appliance
1 Stop service
2 Restore Microsoft Exchange - InfoStore
3 Start service
During restoration, all existing files in the original location will be deleted.Please make sure you have backed up those files if needed.
Start
Cancel

Step 9 The restoration steps are listed, along with a **Start Time** column, a **Duration** column, and an in-progress indicator. The steps are:

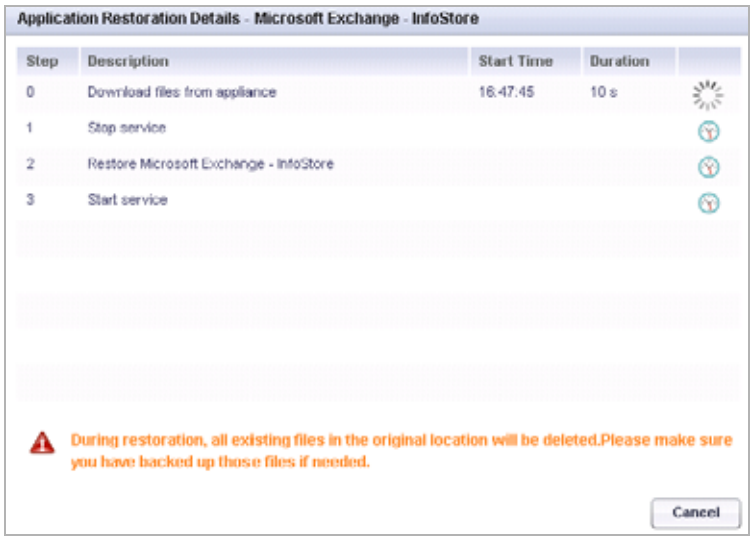
- **Download files from appliance**
- **Stop service**
- **Restore Microsoft Exchange - InfoStore**
- **Start Service**

A warning is also displayed:

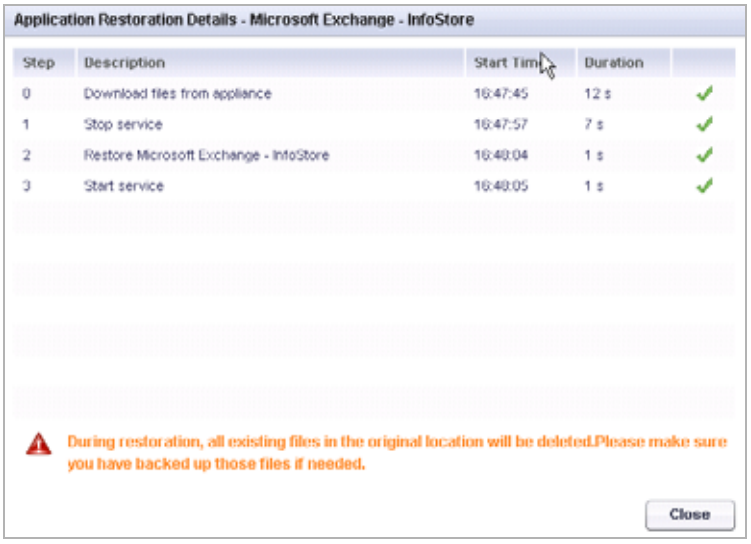
During restoration, all existing files in the original location will be deleted. Please make sure you have backed up those files if needed.

To start the restore process, click **Start**. To exit without restoring any files, click **Cancel**.

The in-progress indicators become active for each step as it is executed, and the **Start Time** and **Duration** values are updated.



Step 10 When the restore is finished, click **Close**.



Note After the data is restored to the Exchange server, you may need to synchronize your local mail client (Outlook) in order to see restored emails.

Recovering an Exchange 2007/2003 User Mailbox

This section describes how to restore an individual user mailbox backup to the Exchange server, by using the Microsoft Exchange User Mailbox Backup and Restore server application in the SonicWALL CDP Agent User Interface.

Note You must log into the agent machine as **cdpadmin** before restoring a User Mailbox. For more information about account privileges to access the Exchange server, see KB821897.

A mailbox must exist in Exchange in order for the restore to work properly. For cases in which the mailbox has been deleted from Exchange, special procedures are necessary.

See the following sections:

- "Restoring the Contents of an Existing Mailbox" on page 182
- "Restoring Deleted Mailboxes in Exchange 2003" on page 183
- "Restoring Deleted Mailboxes in Exchange 2007" on page 183

Restoring the Contents of an Existing Mailbox

To restore an individual user mailbox to the Exchange server, perform the following steps:

Step 1 In the SonicWALL CDP Agent User Interface, click the **My Backups** tab.

Step 2 In the left pane, click **Applications**. The display expands to show available backup tasks.

Step 3 Click the desired backup task. The available revisions are displayed.

Step 4 Click the desired revision. The root folder and details about the revision are displayed, including the date and time.

Step 5 At the bottom right corner, click the Restore icon .

Step 6 In the **Restore Mailbox** dialog box, select the backup that you want to restore. The Application Restoration window opens.

Step 7 In the **Options** drop-down list, select one of the following:

- **Restore to original location** – This option restores the files to the Microsoft Exchange application location.
- **Restore to alternate location** – This option restores the files to the disk of the agent machine.

Step 8 Under **Components**, select the checkboxes for the user mailboxes you want to restore.

Step 9 Click **OK**. The Application Restoration Details window appears.

Step 10 The restoration steps are listed, along with a **Start Time** column, a **Duration** column, and an in-progress indicator. The steps are:

- **Download files from appliance**
- **Stop service**
- **Restore Microsoft Exchange User Mailbox**
- **Start Service**

A warning is also displayed:

During restoration, all existing files in the original location will be deleted. Please make sure you have backed up those files if needed.

To start the restore process, click **Start**. To exit without restoring any files, click **Cancel**.

The in-progress indicators become active for each step as it is executed, and the **Start Time** and **Duration** values are updated.

Step 11 When the restore is finished, click **Close**.

Note After the data is restored to the Exchange server, you may need to synchronize your local mail client (Outlook) in order to see restored emails.

Restoring Deleted Mailboxes in Exchange 2003

Once a mailbox is deleted from Exchange, there is no container to hold the emails, even though SonicWALL CDP has a copy of the mailbox backup. This container (in our case an empty mailbox) must be created prior to restoring the mailbox.

In Exchange 2003, you can either “purge” or “delete” a user mailbox. Mailbox deletion leaves the user account in Exchange, but purging a mailbox removes the user account from Exchange. In either case, the user account in Active Directory still exists (unless removed separately). See the following procedures for each case:

- “Restoring a Deleted Mailbox in Exchange 2003” on page 183
- “Restoring a Purged Mailbox in Exchange 2003” on page 183

Restoring a Deleted Mailbox in Exchange 2003

Step 1 Log in as administrator to the Exchange server.

Step 2 In Exchange, right-click the user mailbox and select **Reconnect**. This reconnects the mailbox to the Active Directory account.

Step 3 Follow the instructions in the procedure “Restoring the Contents of an Existing Mailbox” on page 182 to restore the mailbox.

Restoring a Purged Mailbox in Exchange 2003

Step 1 Obtain the user account information from Active Directory.

Step 2 Use this information to create a new user mailbox in Exchange.

Step 3 Log into the new mailbox via Outlook or Webmail as the user, or have the user log in.

Step 4 Follow the instructions in the procedure “Restoring the Contents of an Existing Mailbox” on page 182 to restore the mailbox.

Restoring Deleted Mailboxes in Exchange 2007

Once a mailbox is deleted from Exchange, there is no container to hold the emails, even though SonicWALL CDP has a copy of the mailbox backup. This container (in our case an empty mailbox) must be created prior to restoring the mailbox.

In Exchange 2007, deleting a user mailbox removes the user account from both Exchange and Active Directory. In this case, there are two methods that can be used to restore a user mailbox. See the following procedures for each case:

- “Restoring a Deleted Mailbox by First Restoring Active Directory” on page 183
- “Restoring a Deleted Mailbox by Creating a New Active Directory Account” on page 184

Restoring a Deleted Mailbox by First Restoring Active Directory

Step 1 Use SonicWALL CDP to restore Active Directory to a version containing the user account.

Step 2 Follow the instructions in the procedure "Restoring the Contents of an Existing Mailbox" on page 182 to restore the mailbox.

Restoring a Deleted Mailbox by Creating a New Active Directory Account

Step 1 Create a new Active Directory user account using the same user name as the deleted account.

Step 2 Create a new user mailbox in Exchange using the same account name and connect to the Active Directory account.

Step 3 Follow the instructions in the procedure "Restoring the Contents of an Existing Mailbox" on page 182 to restore the mailbox.

Note This process might take a long time to complete due to the recovery procedure between Active Directory and Exchange.

Recovering an Exchange 2007/2003 Storage Group

You can restore an Exchange Storage Group by using the SonicWALL CDP Microsoft Exchange InfoStore Backup and Restore server application in the SonicWALL CDP Agent User Interface.

This section describes how to restore an individual Storage Group. You can restore the Storage Group in two ways:

- Restore to Application - Copies the data directly to the Exchange database
- Restore to Disk - Copies the data to a folder on the local disk, then you can copy it to the Exchange database

A storage group must exist in Exchange in order for the restore to work properly. For cases in which the storage group has been deleted from Exchange, special procedures are necessary.

Note The current account must have privileges to access the Exchange server. See KB867704 and KB824126

See the following sections:

- "Restoring a Storage Group" on page 184
- "Restoring Deleted Storage Groups" on page 187

Restoring a Storage Group

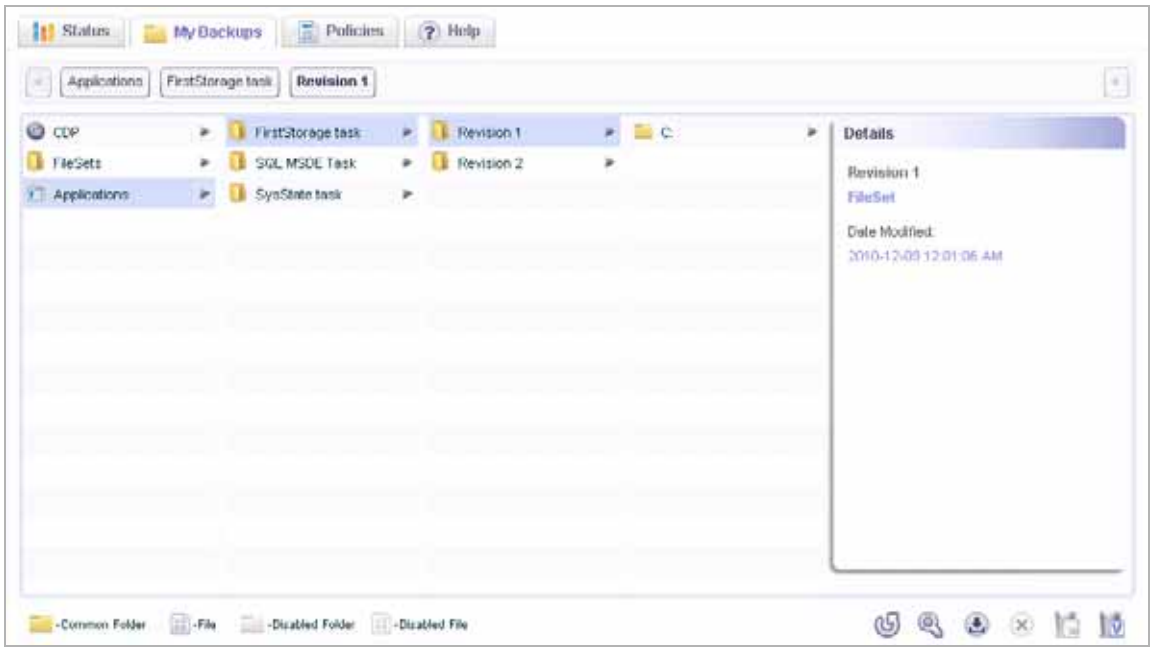
To restore a Storage Group using the SonicWALL CDP Agent User Interface, perform the following steps:

Step 1 In the SonicWALL CDP Agent User Interface, click the **My Backups** tab.

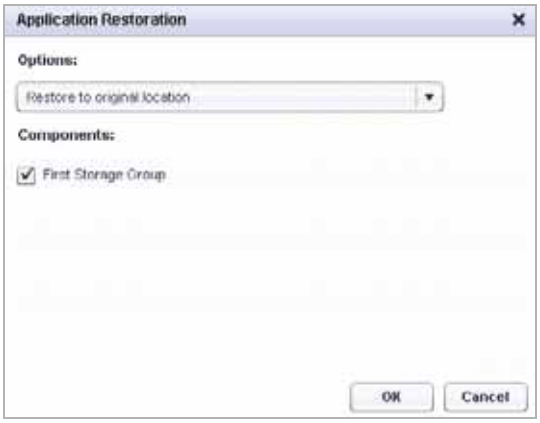
Step 2 In the left pane, click **Applications**. The display expands to show available backup tasks.

Step 3 Click the desired backup task. The available revisions are displayed.

Step 4 Click the desired revision. The root folder and details about the revision are displayed, including the date and time.



Step 5 At the bottom right corner, click the Restore icon . The Application Restoration window opens.

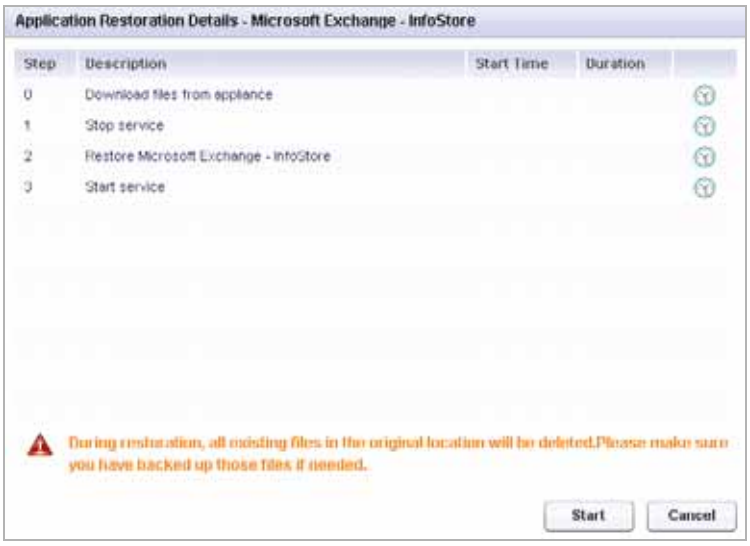


Step 6 In the **Options** drop-down list, select one of the following:

- **Restore to original location** – This option restores the files to the application in their original location in Microsoft Exchange.
- **Restore to alternate location** – This option restores the files to the disk of the agent machine.

Step 7 Under **Components**, select the checkboxes for the storage groups you want to restore.

Step 8 Click **OK**. The Application Restoration Details window appears.



Step 9 The restoration steps are listed, along with a **Start Time** column, a **Duration** column, and an in-progress indicator. The steps are:

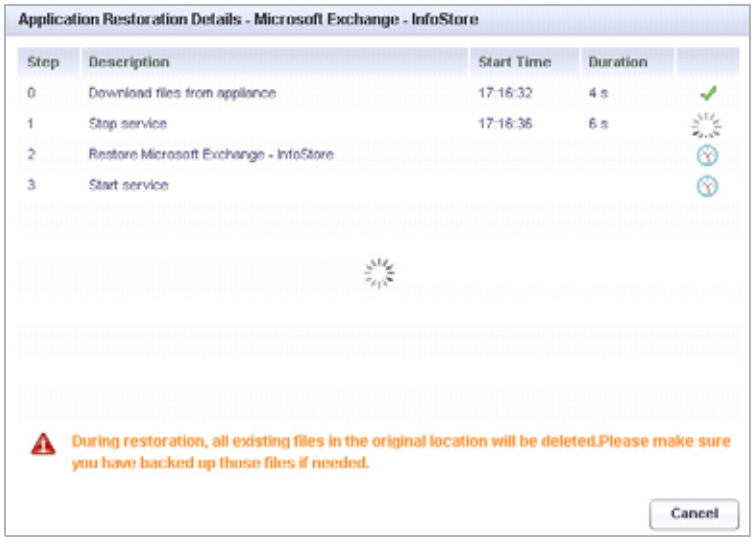
- **Download files from appliance**
- **Stop service**
- **Restore Microsoft Exchange InfoStore**
- **Start Service**

A warning is also displayed:

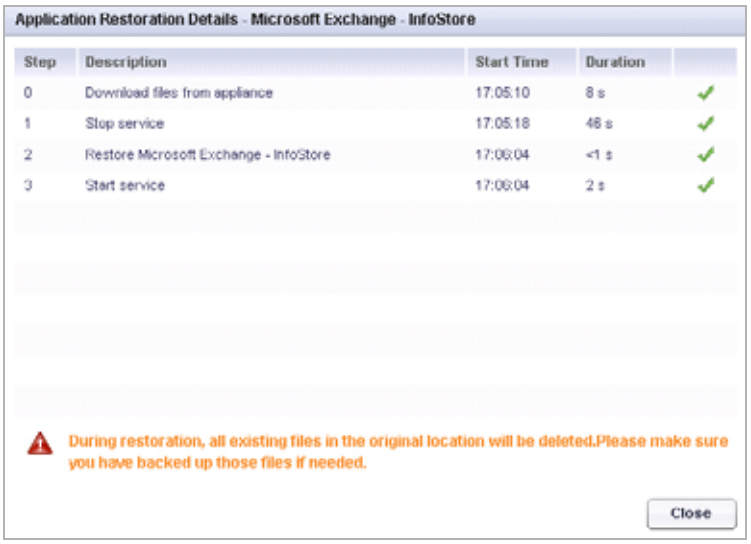
> **During restoration, all existing files in the original location will be deleted. Please make sure you have backed up those files if needed.**

To start the restore process, click **Start**. To exit without restoring any files, click **Cancel**.

The in-progress indicators become active for each step as it is executed, and the **Start Time** and **Duration** values are updated.



Step 10 When the restore is finished, click **Close**.



Note After the data is restored to the Exchange server, you may need to synchronize your local mail client (Outlook) in order to see restored emails.

Restoring Deleted Storage Groups

Once a storage group is deleted from Exchange, there is no container to hold the contents, even though SonicWALL CDP has a copy of the storage group backup. This container (an empty storage group) must be created prior to restoring the storage group.

For both Exchange 2003 and 2007, the recommended way to recover deleted storage groups is to restore Active Directory first and then restore the InfoStore storage group and the user mailboxes. This is because Exchange relies on the Active Directory directory service for its directory operations. Active Directory provides all mailbox information, address list services, and other recipient-related information. Active Directory also stores most Exchange configuration information.

Restoring a Deleted Storage Group, Recommended Method

The recommended method to recover deleted storage groups is to restore Active Directory first and then restore the storage group. This is recommended for both Exchange 2003 and 2007.

Step 1 Use SonicWALL CDP to restore Active Directory to a version containing the storage group.

See the "Recovering System State and Active Directory" section on page 191.

Step 2 Follow the normal steps to restore the storage group with SonicWALL CDP, by using **Restore to original location** to restore files to the application. See "Restoring a Storage Group" on page 184.

Restoring a Deleted Storage Group in Exchange 2003, Alternate Method

This method does not involve restoring Active Directory first, and is available as an alternate method for Exchange 2003, but not for Exchange 2007. In Exchange 2007, when you delete a user mailbox from the Exchange Management Console, the user is also deleted from Active Directory.

If you restore a deleted storage group with this method, there will be two instances of **SMTP** and **SystemMailbox** under <Storage Group>/<Mailbox Store>/Mailboxes after the restore.

One instance of **SMTP** and **SystemMailbox** is created when you re-create the Mailbox store. This pair has a new ID number. The other instance is from the SonicWALL CDP restore of the storage group. This pair has the original ID number.

Despite the duplicate mailbox pair, there are no problems when sending or receiving emails or when backing up or restoring the original (restored) storage group.

Step 1 Log in as administrator to the Exchange server.

Step 2 Select one backup revision of your deleted storage group, then choose **Restore to alternate location** to restore the files to disk.

Step 3 Browse to the restored folder **Backup0001**, find the ***.edb** files.

Step 4 Create a new storage group with the same name as the one backed up in SonicWALL CDP.

Step 5 Create a new mailbox database for each **.edb** file.

For example, if there are two .edb files:

- Mailbox Database1.edb
- Mailbox Database2.edb

Then create two new mailbox databases using these same names ("Mailbox Database1.edb" and "Mailbox Database2.edb") under the newly created storage group.

Step 6 Follow the normal steps to restore an InfoStore storage group by using **Restore to original location** to restore the files to the application. See “Restoring a Storage Group” on page 184.

Step 7 After the storage group is restored, open the Exchange system manager and **Reconnect** the user mailboxes.

Recovering SharePoint

Recovery of data from Microsoft SharePoint using SonicWALL CDP allows users to retrieve SharePoint SQL database revisions from agent machines previously configured to backup those databases. When restoring SharePoint databases from a SonicWALL CDP backup, you need to restore all databases in the backup revision to provide a consistent environment. SharePoint data cannot be restored from the Web Management Interface.

Note SharePoint data can only be restored using the Agent User Interface.

To recover SharePoint data from the SonicWALL CDP appliance, perform the following steps:

Step 1 Launch the **SonicWALL CDP Agent** software on the agent machine on which you want to recover the SharePoint data.

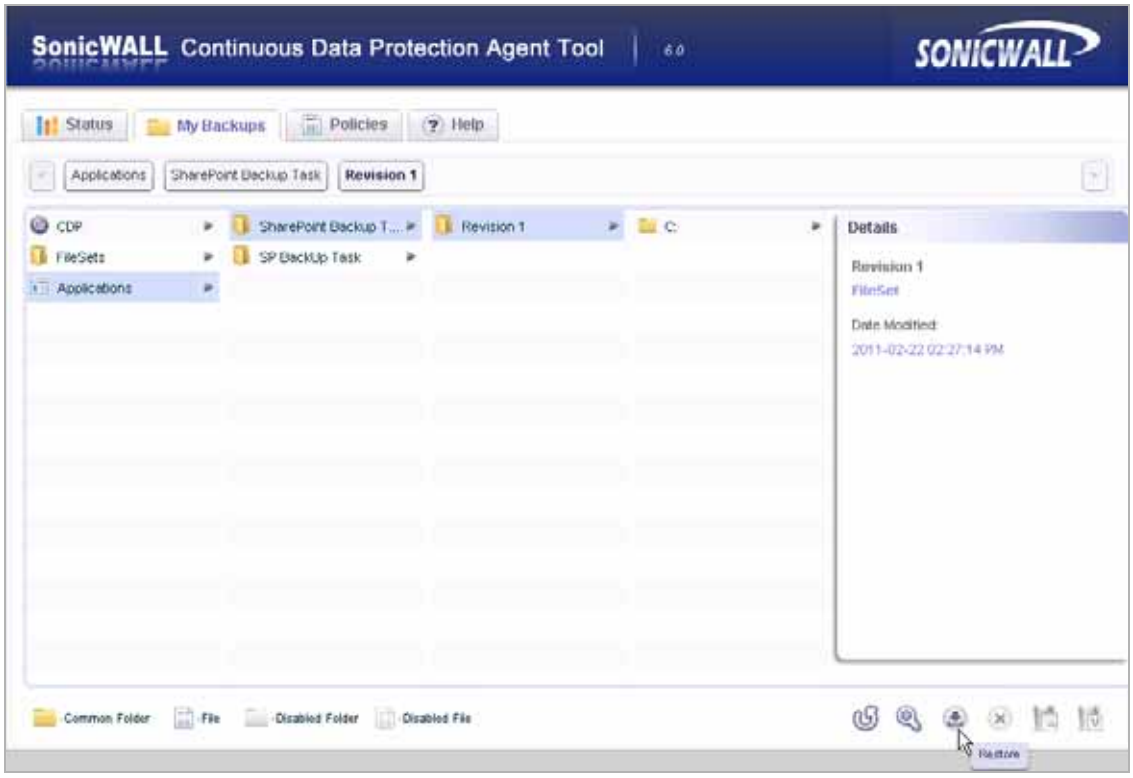
Step 2 If necessary, click the Change Appliance icon to change the SonicWALL CDP appliance to the one with the files you need.

Step 3 Click the **My Backups** tab.

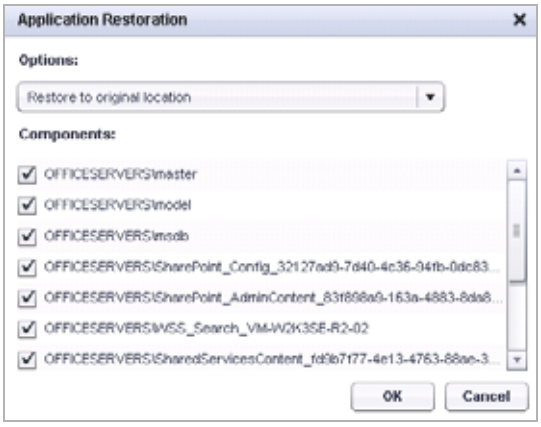
Step 4 In the left pane, click **Applications**. The display expands to show available backup tasks.

Step 5 Click the desired backup task. The available revisions are displayed.

Step 6 Click the desired revision. The root folder and details about the revision are displayed, including the date and time.



Step 7 At the bottom right corner, click the Restore icon . The Application Restoration window opens.



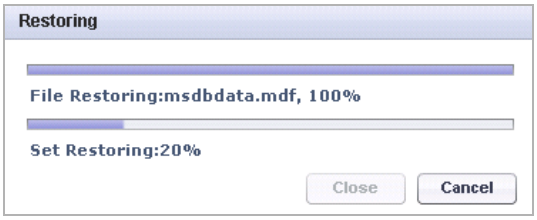
Step 8 In the **Options** drop-down list, select one of the following:

- **Restore to original location** – restore the database files on top of the original files
- **Restore to alternate location** – restore the database files to another location on disk

  Use this option if you want to verify the files, then copy them to the original location either manually or by using a separate tool or application. You can browse to the folder where you want the data restored, or create a new folder.

Step 9 Click **OK** to begin the restoration. Click **Cancel** to exit without restoring the files.

The Restoring window displays the progress of the restore.



Step 10 When the restore process is finished, the Restoring window changes to Done. Click the **Close** button to close the window.

Recovering System State and Active Directory

Recovery of data from System State and Active Directory using SonicWALL CDP allows users to retrieve Active Directory revisions from agent machines previously configured to backup that data. When restoring Active Directory from a SonicWALL CDP backup, you need to restore all associated, interdependent System State files to provide a consistent environment. Active Directory data cannot be restored from the Web Management Interface.

Note Active Directory data can only be restored using the Agent User Interface.

This section contains the following subsections:

- "Restarting the Domain Controller in Safe Mode" section on page 191
- "Restoring Active Directory and System State" section on page 192
- "Using Authoritative Restore" section on page 195

Restarting the Domain Controller in Safe Mode

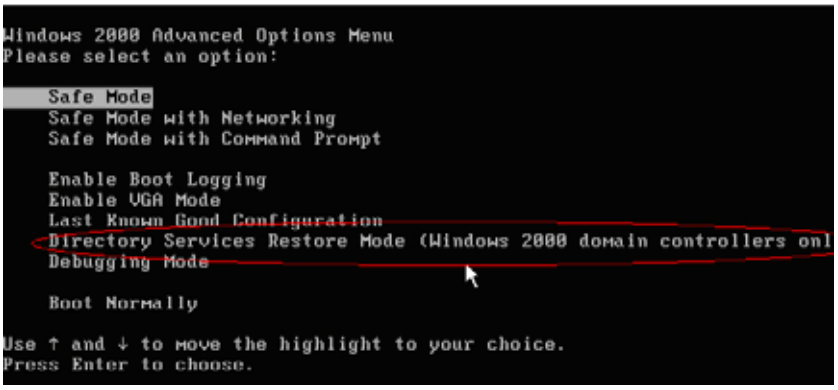
With the exception of Active Directory on Windows Server 2008, you cannot restore Active Directory in normal Windows mode. This is because the service is already active. Before restoring Active Directory on Windows Server 2003 or 2000, you must boot your computer into safe mode. Once in safe mode, you can restore the Active Directory as an application. This is because in safe mode the Active Directory is disabled.

Note Do not boot your computer into safe mode when restoring Active Directory on Windows Server 2008 or higher.

To boot your computer into safe mode, perform the following steps:

Step 1 Boot your computer and press **F5** or **F8** after POST/BIOS and before the Windows splash-screen, depending on hardware specs of the server.

Step 2 Select the **Directory Services Restore Mode (DSRM)**.


Windows 2000 Advanced Options Menu
Please select an option:
Safe Mode
Safe Mode with Networking
Safe Mode with Command Prompt
Enable Boot Logging
Enable VGA Mode
Last Known Good Configuration
Directory Services Restore Mode (Windows 2000 domain controllers onl
Debugging Mode
Boot Normally
Use ↑ and ↓ to move the highlight to your choice.
Press Enter to choose.

Step 3 Login as Restore Mode Administrator.

Restoring Active Directory and System State

Restoring Active Directory will cause the loss of any changes to Active Directory since the date of the backup that is being restored.

SonicWALL recommends the use of redundant Active Directory domain controllers. In the case of mirrored Active Directory domain controllers, you can optionally restore a small part of the database rather than the entire database (for example, because some people were deleted by mistake by the administrator or a script/program), keeping the remainder of the database up to date. In this case, the administrator selects the old data that needs to be pushed on top of the latest data during replication, after the server (2003/2000 only) is rebooted out of Recovery Mode.

Restoration steps can be different depending on the computer's operating system and configuration.

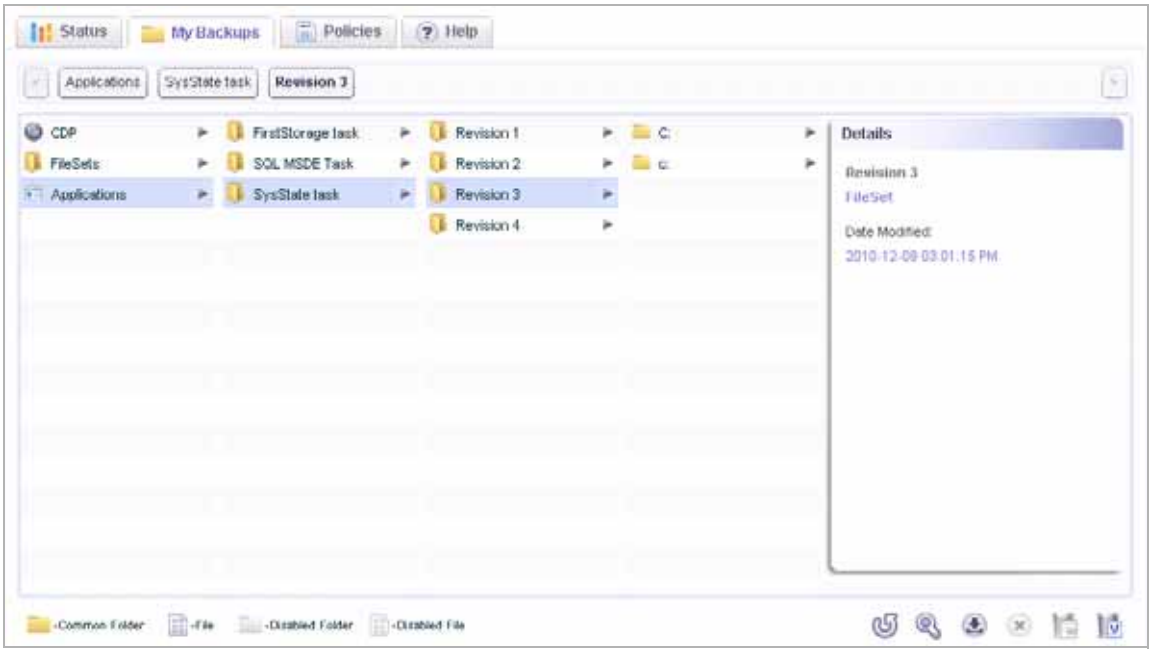
To restore System State and Active Directory using the SonicWALL CDP Agent User Interface, perform the following steps:

Step 1 In the SonicWALL CDP Agent User Interface, click the **My Backups** tab.

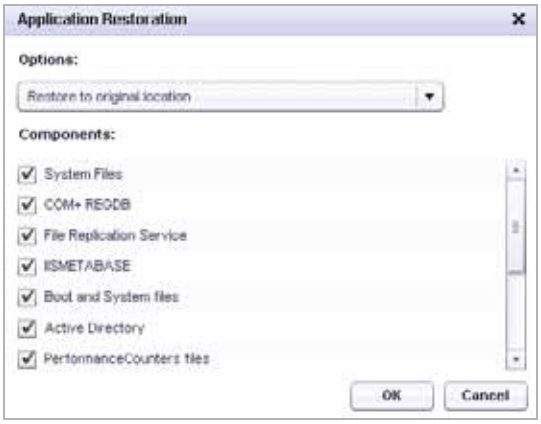
Step 2 In the left pane, click **Applications**. The display expands to show available backup tasks.

Step 3 Click the desired backup task. The available revisions are displayed.

Step 4 Click the desired revision. The root folder and details about the revision are displayed, including the date and time.



Step 5 At the bottom right corner, click the Restore icon . The Application Restoration window opens.



Step 6 In the **Options** drop-down list, select one of the following:

- **Restore to original location** – This option restores the files to the application in their original location, and to original System State file locations.
- **Restore to alternate location** – This option restores the files to the disk of the agent machine.

Step 7 Under **Components**, select the checkboxes for the files you want to restore. To ensure a consistent environment after the restore, select all files.

It is not recommended to restore certain System State subcomponents individually (like Certificate Services database, and COM+ Class Registration database) due to dependencies. For more information, see:

http://technet.microsoft.com/en-us/library/cc785306%28WS.10%29.aspx

Step 8 Click **OK**. The Application Restoration Details window appears.

Application Restoration Details - System State
Step
Description
Start Time
Duration
0 Download files from appliance
1 Restore Windows Boot Files
2 Restore Windows System Files
3 Restore Windows Performance Counters Files
4 Restore Windows Internet Information Services Metabase
5 Reboot Windows with Active Directory Repair Mode
6 Restore Windows COM+ Class Registration Database
7 Restore Windows File Replication Service
8 Restore Windows Active Directory Domain Services (NTDS
9 Restore Windows Registry
10 Reboot Windows with Normal Mode
Start
Cancel

Step 9 The restoration steps are listed, along with a **Start Time** column, a **Duration** column, and an in-progress indicator. The steps are:

- **Download files from appliance**
- **Restore Windows Boot Files**
- **Restore Windows System Files**
- **Restore Windows Performance Counters Files**
- **Restore Windows Internet Information Services Metabase**
- **Reboot Windows with Active Directory Repair Mode**
- **Restore Windows COM+ Class Registration Database**
- **Restore Windows File Replication Service**
- **Restore Windows Active Directory Domain Services (NTDS)**
- **Restore Windows Registry**
- **Reboot Windows with Normal Mode**
- **Restore Windows Management Instrumentation (WMI)**
- **Restore Windows Event Log**
- **Reboot Windows**

To start the restore process, click **Start**. To exit without restoring any files, click **Cancel**.

The in-progress indicators become active for each step as it is executed, and the **Start Time** and **Duration** values are updated.

Application Restoration Details - System State
Step
Description
Start Time
Duration
0 Download files from appliance 08:57:55 463 s
1 Restore Windows Boot Files 09:05:38 <1 s
2 Restore Windows System Files 09:05:38 35 s
3 Restore Windows Performance Counters Files
4 Restore Windows Internet Information Services Metabase
5 Reboot Windows with Active Directory Repair Mode
6 Restore Windows COM+ Class Registration Database
7 Restore Windows File Replication Service
8 Restore Windows Active Directory Domain Services (NTDS
9 Restore Windows Registry
10 Reboot Windows with Normal Mode
Cancel

Step 10 When the **Reboot Windows with Active Directory Repair Mode** step is reached, the restore process pauses and prompts you to select one of the following options:

- **Run MSConfig** – Click this button to continue with the reboot. The SonicWALL CDP Agent exits and must be restarted.

  MSConfig is a utility that is configured by SonicWALL CDP to perform a diagnostic startup. It can also be used to modify which programs run at startup, edit certain configuration files, and control Windows services.

- **Run Later** – Click this button to stop the restore process and return to the previous screen in the SonicWALL CDP Agent User Interface.

Application Restoration Details - System State
Step
Description
Start Time
Duration
0 Download files from appliance 08.57.55 483 s
1 Restore Windows Boot Files 09.05.38 <1 s
2 Restore Windows System Files 09.05.38 42 s
3 Restore Windows Performance Counters Files 09.06.20 <1 s
4 Restore Windows Internet Information Services Metabase 09.06.20 <1 s
5 Reboot Windows with Active Directory Repair Mode 09.06.20 1 s
6 Restore Windows COM+ Class Registration Database
7 Restore Windows File Replication Service
8 Restore Windows Active Directory Domain Services (NTDS
9 Restore Windows Registry
10 Reboot Windows with Normal Mode
Run MSConfig
Run Later

Step 11 When the restore is finished, click **Close**.

Using Authoritative Restore

An authoritative restore is most commonly used to restore corrupt or deleted objects. For example, a deleted user account can be recovered from an Active Directory backup that precedes the deletion of the user account. An authoritative restore should not be used to restore an entire domain controller, nor should it be used as part of a change-control infrastructure.

Proper delegation of administration and change enforcement will optimize data consistency, integrity, and security.

MSDN Web links:

- http://support.microsoft.com/?kbid=258062
- http://support.microsoft.com/default.aspx?scid=kb;en-us;240655
- http://support.microsoft.com/default.aspx?scid=kb;en-us;830574
- http://support.microsoft.com/default.aspx?scid=kb;en-us;314980
- http://support.microsoft.com/default.aspx?scid=kb;en-us;265089
- http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/Operations/f66ee9e4-96d7-4f74-a2fe-d669194bf5a2.mspx

MSDN Engineering recommends the following as the most helpful to see what is happening:

- http://support.microsoft.com/default.aspx?scid=kb;en-us;840001
- http://support.microsoft.com/kb/239803/

Recovering Data from Microsoft SQL Server

Recovery of data from Microsoft SQL using SonicWALL CDP allows users to retrieve Microsoft SQL revisions from an agent machine previously configured to backup that data. Microsoft SQL recovery can be made directly to the SQL database.

Restoring the database can be done in two ways. The database can be either restored to disk or to application. When restoring the database to disk, the database is downloaded as a set of files from the SonicWALL CDP Appliance.

Restoring to application, on the other hand, applies the database directly to the same SQL server.

If an SQL database system fails, the first step is to recover all databases and transaction log files from the server. These databases contain the latest information, up to the point of failure. Next, the SQL system should be brought up on the same server or a different server. Having spare hardware will speed up database recovery.

Each recovered database should be run through a data consistency check (using “DBCC CHECKDB”) because it is possible that these are corrupted databases and may have been the reason for failure. If the databases are corrupted, these could either be fixed, which normally includes data loss, or the latest backed up database (from CDP) could be used instead.

See the following sections:

- “Recovering SQL Using the Agent User Interface” section on page 196
- “Additional Information” section on page 199

Recovering SQL Using the Agent User Interface

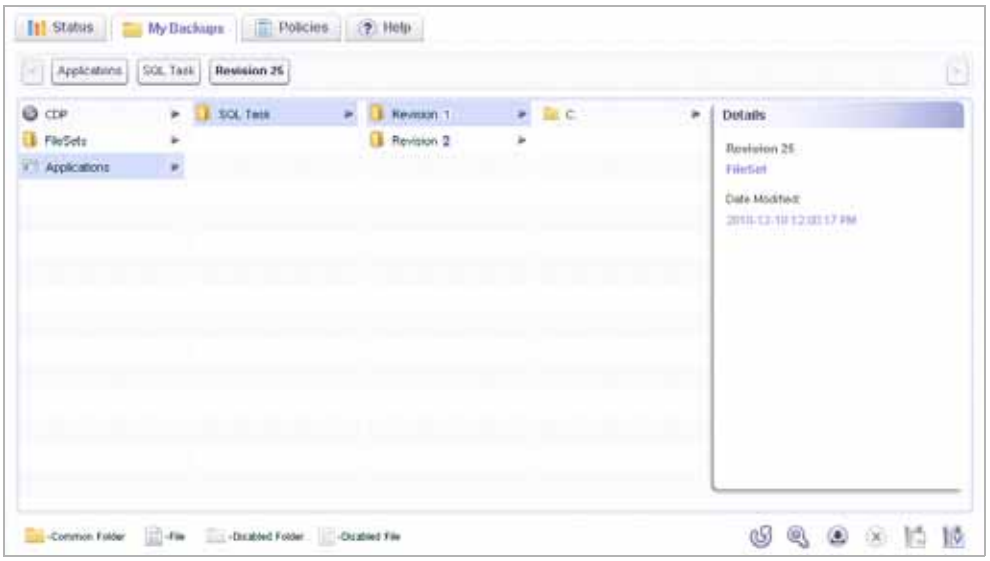
To restore Microsoft SQL databases using the SonicWALL CDP Agent User Interface, perform the following steps:

Step 1 In the SonicWALL CDP Agent User Interface, click the **My Backups** tab.

Step 2 In the left pane, click **Applications**. The display expands to show available backup tasks.

Step 3 Click the desired backup task. The available revisions are displayed.

Step 4 Click the desired revision. The root folder and details about the revision are displayed, including the date and time.



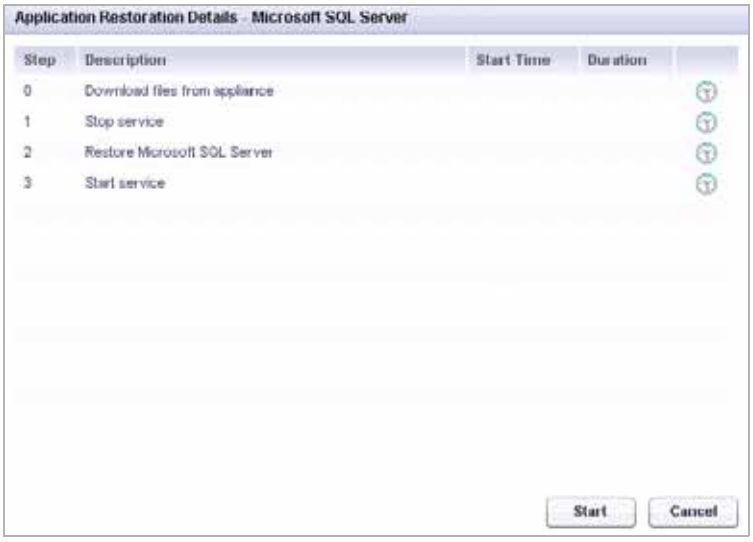
Step 5 At the bottom right corner, click the Restore icon . The Application Restoration window opens.

Step 6 In the **Options** drop-down list, select one of the following:

- **Restore to original location** – This option restores the files to the application in their original location for Microsoft SQL.
- **Restore to alternate location** – This option restores the files to the disk of the agent machine.

Step 7 Under **Components**, select the checkboxes for the databases you want to restore.

Step 8 Click **OK**. The Application Restoration Details window appears.

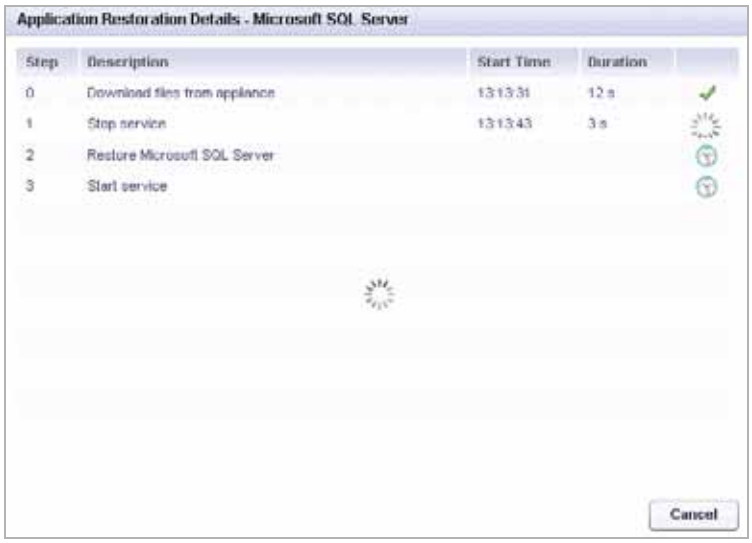


Step 9 The restoration steps are listed, along with a **Start Time** column, a **Duration** column, and an in-progress indicator. The steps are:

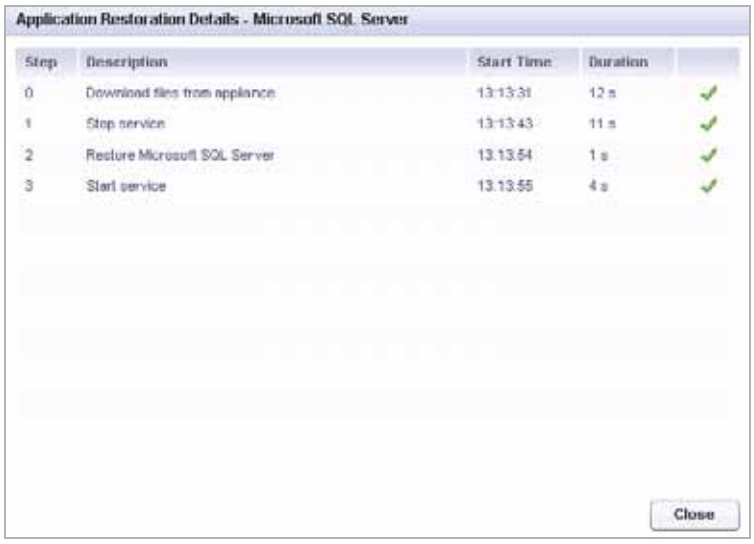
- **Download files from appliance**
- **Stop service**
- **Restore Microsoft Exchange SQL Server**
- **Start Service**

To start the restore process, click **Start**. To exit without restoring any files, click **Cancel**.

The in-progress indicators become active for each step as it is executed, and the **Start Time** and **Duration** values are updated.



Step 10 When the restore is finished, click **Close**.



Additional Information

More information can be found here:

SQL Forum on Disaster Recovery run by Microsoft: http://forums.microsoft.com/MSDN/ShowForum.aspx?ForumID=744&SiteID=1

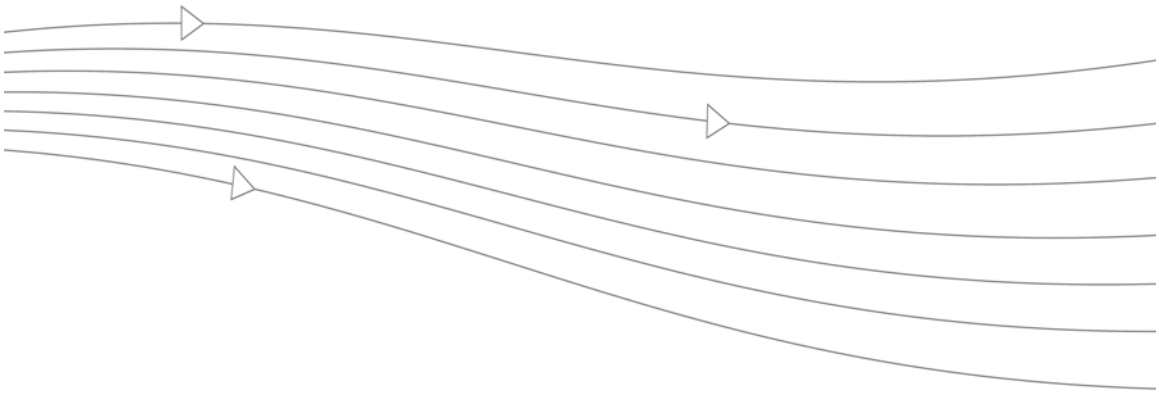
Handling Large Log Files: http://mkruger.cfwebtools.com/index.cfm?mode=entry&entry=CFEA536D-FC85-271F-691D1A974BA71B07

Database Locked Error

Actions that can lock the database and prevent the restore process include:

- Querying
- Accessing by user or application
- Opening Web Management Interface with database selected

Revisions may not appear immediately or even for some time due to a number of reasons including, but not limited to, large databases, single user mode databases, 24x7 databases, or other databases with high access frequency.



Chapter 12: Configuring Site-to-Site Backup and Recovery

The SonicWALL CDP Site-to-Site Data Backup Service is an optional offsite backup and recovery solution that stores data in a secure data center. In the event of a disaster that has rendered local data corrupted or destroyed, data can be recovered from the Site-to-Site Service. You can manage and recover offsite data at any time; a disaster is not required.

This chapter provides an overview of the SonicWALL CDP Site-to-Site Service concepts and configuration guidelines. This chapter includes the following sections:

- "Site-to-Site Service Overview" section on page 201
- "Preparing for the Site-to-Site Service" section on page 205
- "Configuring the Downstream CDP Appliance" section on page 208
- "Configuring the Upstream CDP Appliance Quota" section on page 209
- "Removing a Downstream CDP" section on page 209
- "Selecting Files for Offsite Backup" section on page 210
- "Recovering Data From the Upstream Appliance" section on page 210
- "Deleting Data From the Upstream Appliance" section on page 212
- "Replacing the Downstream CDP Appliance" section on page 212

Site-to-Site Service Overview

This section provides an introduction to the SonicWALL CDP Site-to-Site Service feature. This section contains the following subsections:

- "What is the Site-to-Site Service?" section on page 202
- "Benefits of the Site-to-Site Service" section on page 202
- "How Does the Site-to-Site Service Work?" section on page 203

What is the Site-to-Site Service?

The SonicWALL CDP Site-to-Site Data Backup Service is an optional offsite backup and recovery solution that stores data in a secure data center, and can be purchased for an additional fee. For more information, see the SonicWALL CDP Offsite Data Backup Service data sheet at: <http://www.sonicwall.com/downloads/DS_CDP_Offsite_US_060507.pdf>.

The CDP Site-to-Site Service feature provides a secure, reliable, and confidential method of backing up and recovering data from one or more local CDP appliances to another local or offsite CDP appliance.

In a typical one-to-one configuration of CDP Site-to-Site, one local CDP appliance, or downstream appliance, is used to backup local workstations. A second CDP appliance, or upstream appliance, is deployed locally or at a remote location and is used to backup the downstream CDP appliance.

Note You must purchase an 8x5 or 24x7 support contract and a 1, 3, 5, or 10 node Offsite license for the upstream CDP appliance.

The one-to-one CDP Site-to-Site configuration can be expanded to include multiple downstream CDP appliances that back up to a single local or offsite upstream CDP appliance. The upstream appliance needs to have sufficient Offsite nodes licensed.

Note Multiple downstream CDP appliances can backup to a single upstream CDP appliance. Upstream CDP appliances can also backup local data to the SonicWALL Offsite Portal or to yet another CDP appliance. However, this third appliance cannot send any data offsite.

In the event that a downstream CDP appliance is rendered unusable, the CDP Site-to-Site feature allows you to recover your data, settings and configurations directly from the upstream CDP appliance. If the data on the upstream CDP appliance is not the most recent, choose the option to only download settings and configurations; the local agents will then back up the most recent data to the downstream CDP appliance which will be sent to the upstream CDP appliance. If the upstream CDP appliance is rendered unusable, it can easily be replaced with a new CDP appliance configured with the same IP address as the original upstream CDP appliance.

Benefits of the Site-to-Site Service

The benefits of the SonicWALL CDP Site-to-Site feature include:

- Secure, confidential data backup and recovery
- Additional protection against data loss
- Easy deployment
- Quick recovery of settings and configurations or complete recovery of data, settings, and configurations.

How Does the Site-to-Site Service Work?

The CDP Site-to-Site feature requires a minimum of two CDP appliances to be deployed in a one-to-one scenario, in which a single upstream CDP appliance is the backup method for a downstream CDP appliance. The upstream CDP appliance can be deployed locally or offsite using a VPN or WAN connection, as illustrated in Figure 1 and Figure 2. The downstream CDP appliance must be configured to backup to the IP address of the upstream CDP appliance, and the upstream CDP appliance must be licensed for Offsite and have at least one node available.

Multiple downstream CDP appliances can be configured to backup to a single local or offsite upstream CDP appliance in a many-to-one configuration. Upstream CDP appliances can also be used as a backup method for local agents, and can back up the local agent data to the SonicWALL offsite portal or to another CDP. Data, settings and configuration backed up from the downstream CDP appliance to the upstream CDP appliance are 256-bit encrypted and compressed, and sent using port 2022. All other features, including alerts, policies, and reports, can be configured on the upstream and downstream CDP appliances.

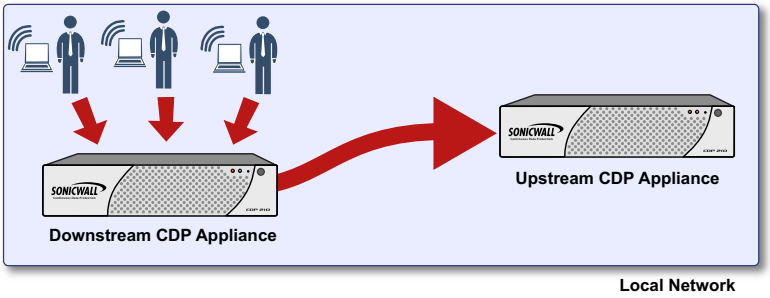
In the event of a disaster, data, settings, and configurations (or just settings and configurations) can be recovered from the upstream CDP appliance to the downstream CDP appliance. If the data on the upstream appliance is outdated, the option to recover only settings and configurations provides the ability to rapidly set up the replacement CDP. The replacement will then recover the latest data directly from its local agents, and then pass this data on to the upstream CDP appliance, thereby reinstating full backup protection.

If the downstream CDP appliance is rendered unusable, it is necessary to obtain a new downstream CDP appliance to replace it. The upstream CDP appliance must be notified of the change and the new box must be configured to backup to it prior to recovering data from the upstream CDP appliance.

Sample Setup Cases

The diagram in Figure 1 provides an example of a one-to-one CDP Site-to-Site deployment. Multiple agents are configured to backup to the downstream CDP appliance (IP address 10.0.0.1). The downstream CDP appliance is configured to backup to the local upstream CDP appliance (IP address 10.0.0.2).

Figure 1 CDP Site-to-Site: One to One Local Configuration



The diagram in Figure 2 provides an example of a one-to-one offsite CDP Site-to-Site deployment. Multiple agents are configured to backup to the downstream CDP appliance (IP

address 10.0.0.1). The downstream CDP appliance is configured to backup to the offsite upstream CDP appliance (IP address 10.1.1.2) using a VPN or WAN connection.

Figure 2 CDP Site-to-Site: One to One Offsite Configuration

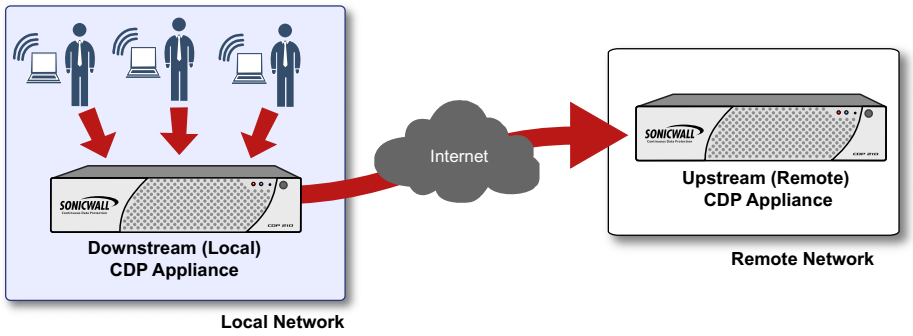
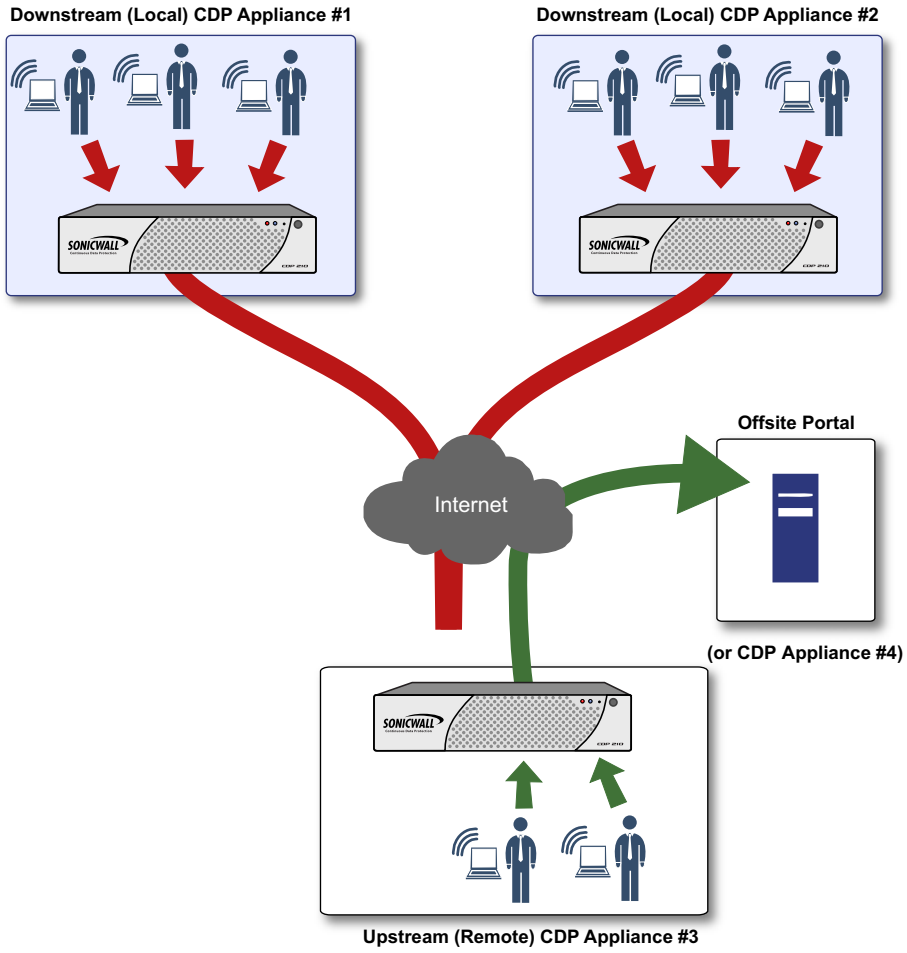


Figure 3 provides an example of a many-to-one CDP Offsite deployment with multiple CDP appliances (IP addresses 10.0.0.1 and 10.0.0.3) configured to backup to a single upstream CDP appliance (IP address 10.1.1.2). The upstream CDP appliance can be used to backup local clients and backup this data either to the offsite portal or to a final CDP.

Note Only data being backed up by the upstream CDP's local clients will be sent to the offsite portal. If the data is sent to another CDP, this final CDP cannot send any data offsite.

Figure 3 CDP Offsite: Many to One Configuration; Single Destination Backup



Preparing for the Site-to-Site Service

This section contains the following sub-sections:

- "Site-to-Site Service Best Practices" section on page 205
- "Administrator Prerequisites" section on page 206
- "Purchasing Licenses and Support" section on page 206

Site-to-Site Service Best Practices

For best performance, SonicWALL recommends you follow these practices:

- Seed data to a second local CDP when dealing with large data sets.
- Consider having a dedicated Internet connection for many-to-one backup scenarios.
- Separate out data being uploaded: Do not seed all machines at once. Do not seed all files from a single large machine at one time.

- No circular references of data. An upstream appliance cannot back up to one of its downstream appliances.

Administrator Prerequisites

The following deployment prerequisites are required to use the CDP Site-to-Site feature:

- Two or more CDP appliances running 6.0 or higher firmware
- 8x5 or 24x7 support contract for the upstream CDP Appliance
- Offsite license for the upstream CDP appliance to accept downstream CDP appliance connections
- IP address or Fully Qualified Domain Name for the Upstream CDP Appliance
- In the case of an offsite Upstream Appliance, port 2022 must be open to receive incoming traffic within firewall rules.

Note You must purchase an 8x5 or 24x7 support contract and a 1, 3, 5, or 10 node Offsite license for the upstream CDP appliance.

Purchasing Licenses and Support

Note Your SonicWALL CDP appliances must be registered before they can be deployed for Site-to-Site. Refer to the *SonicWALL CDP Getting Started Guide* for further information on registering your appliances.

You must purchase an 8x5 or 24x7 support contract and a 1, 3, 5, or 10 node Offsite license for the upstream CDP appliance. This can be done directly through mysonicwall.com or through your reseller.

To configure the upstream CDP appliance to accept backup data from the downstream CDP appliance, perform the following steps:

Step 1 Open a Web browser on the computer you are using to manage the SonicWALL SSL VPN.

Step 2 Enter **http://www.mysonicwall.com** in the **location** or **address** field.

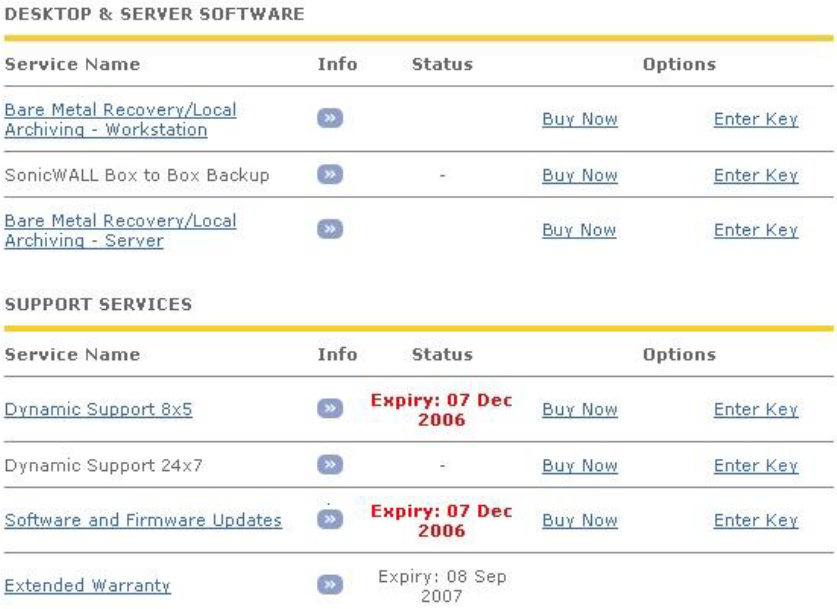
The **mySonicWALL.com login** page is displayed.

Step 3 Enter your mySonicWALL.com account **username** and **password** in the appropriate fields and click the **submit** button.

Step 4 Navigate to **My Products** in the left-hand navigation bar

Step 5 Select the CDP appliance you wish to use as the Upstream backup.

Step 6 Register for a Dynamic Support license.



DESKTOP & SERVER SOFTWARE

Service Name	Info	Status	Options	
Bare Metal Recovery/Local Archiving - Workstation	»		Buy Now	Enter Key
SonicWALL Box to Box Backup	»	-	Buy Now	Enter Key
Bare Metal Recovery/Local Archiving - Server	»		Buy Now	Enter Key

SUPPORT SERVICES

Service Name	Info	Status	Options	
Dynamic Support 8x5	»	Expiry: 07 Dec 2006	Buy Now	Enter Key
Dynamic Support 24x7	»	-	Buy Now	Enter Key
Software and Firmware Updates	»	Expiry: 07 Dec 2006	Buy Now	Enter Key
Extended Warranty	»	Expiry: 08 Sep 2007		

Step 7 Register for an Offsite Node Support license.

Note Offsite Node licenses do not expire. You may add additional Node Licenses by purchasing them from the mysonicwall.com Website.

Step 8 Login to your upstream CDP appliance's Web management interface.

Step 9 Navigate to the **Licenses** page in the left-hand navigation bar.

Step 10 Click the **Refresh** button to have the CDP appliance update its license.

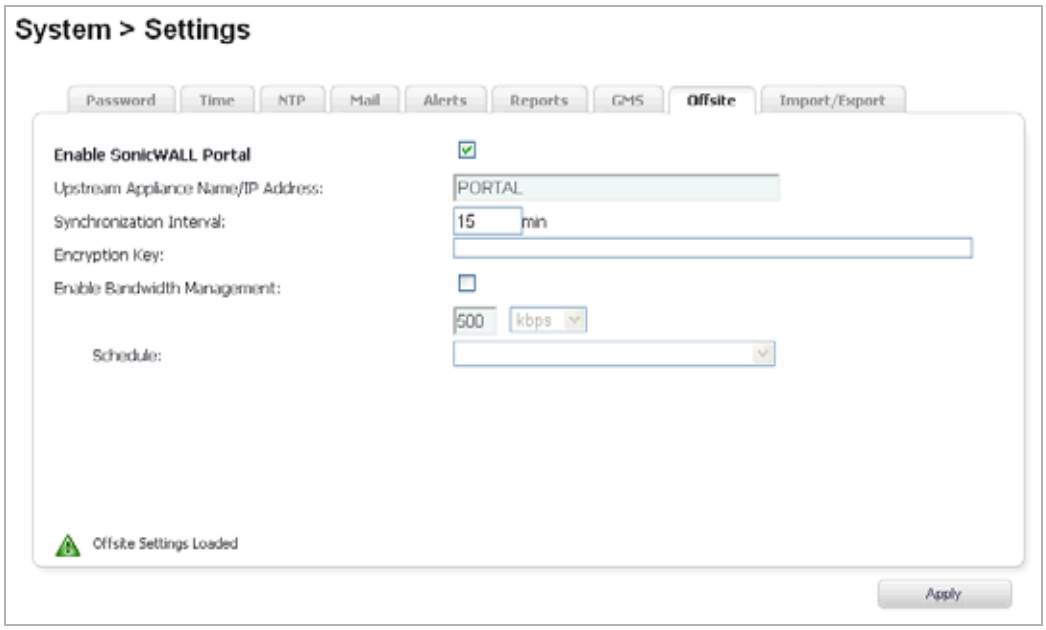
The appliance should now show the correct number of nodes licensed and is ready to backup a downstream CDP appliance.

Configuring the Downstream CDP Appliance

To configure the downstream CDP appliance to back up to the SonicWALL CDP Portal or to an upstream CDP appliance, perform the following steps:

Step 1 Login to the downstream CDP appliance using the Web Management Interface.

Step 2 Navigate to the **System > Settings** page and select the **Offsite** tab.



Step 3 To use the SonicWALL Portal as the upstream destination, leave the **Enable SonicWALL Portal** checkbox selected and leave **PORTAL** in the **Upstream Appliance Name/IP Address** field.

Step 4 To use another SonicWALL CDP appliance as the upstream destination, clear the checkbox next to **Enable SonicWALL Portal** and type the IP address or the FQDN (Fully Qualified Domain Name) of the upstream CDP appliance in the **Upstream Appliance Name/IP Address** field.

Note It is important that the upstream and downstream appliances have different IP addresses. Refer to the *SonicWALL CDP Getting Started Guide* for further information on configuring an appliance's IP address and domain name.

Step 5 Set the desired number of minutes in the **Synchronization Interval** field. The default, and minimum, is 15 minutes. To save bandwidth, you can set the interval to a larger number for less frequent synchronization between the downstream and upstream appliances..

Step 6 The **Encryption Key** is set automatically, and cannot be changed. If you switch between the Portal and another upstream destination, you will see a different key in this field. You can copy the key to your computer clipboard and save it in a text file for secure storage offsite.

Step 7 To specify the maximum bandwidth used during synchronization with the upstream destination, select the **Enable Bandwidth Management** checkbox, enter the desired numerical value in the field below it, and select **kbps**, **Mbps**, or **Gbps** as the units.

Step 8 To enforce a schedule for bandwidth management to the upstream destination, select the **Enable Bandwidth Management** checkbox and then select the desired schedule from the **Schedule** drop-down list. You can configure an appropriate schedule on the **Policy > Schedules** page.

When the schedule for Bandwidth Management is in the “off” period, SonicWALL CDP will use all available offsite bandwidth to synchronize data.

Step 9 Click **Apply**.

Configuring the Upstream CDP Appliance Quota

The SonicWALL CDP Site-to-Site Data Backup provides different services, ranging from 5 to 100 GB of quota. The quota is the maximum amount of data that can be backed up. You need to make sure that the total size of all of your backups does not exceed the quota limit. If quota is exceeded, a subsequent backup will fail, the **Quota Exceeded Error** message will be displayed, and the status for the last backup will change to **Quota Exceeded**. You will receive an email notification informing you of the failed backup attempt. You can free up your storage space by removing some of the old backups, or you can purchase additional quota.

For information about editing the default policy quota or creating a custom policy with a custom quota, refer to the “Creating a Global Policy” section on page 82.

To apply a quota for the amount of data the upstream CDP appliance will accept from the downstream CDP appliance, perform the following steps:

Step 1 Login to the upstream CDP appliance using the Web Management Interface.

Step 2 Navigate to the **Agents > Manage** page.

Step 3 Click the **Policy** tab.

Step 4 In the left pane, under the **SonicWALL CDP Agents** list, select the downstream CDP appliance.

Step 5 Click the **Edit** icon for the downstream CDP appliance.

Step 6 From the **Select Admin Policy** drop-down list, select the **Default Policy**, or, if you have configured one, a custom policy with a specific quota defined.

Step 7 Click **OK**.

Removing a Downstream CDP

Removing a downstream CDP will delete all the relevant backup data from the upstream CDP appliance. To remove a downstream CDP and free up an upstream node, perform the following steps:

Step 1 Login to the downstream CDP appliance using the Web Management Interface.

Step 2 Navigate to the **System > Settings** page and select the **Offsite** tab.

Step 3 Clear the **Upstream Appliance Name/IP Address** field.

Step 4 Click **Apply**.

Step 5 Login to the upstream CDP appliance using the Web Management Interface

Step 6 Navigate to the **Agents > Manage** page.

Step 7 Click the **Configure** tab.

Step 8 Click the **Delete** icon for the downstream CDP appliance.

Step 9 An alert displays. Click **Yes**.

Selecting Files for Offsite Backup

Once properly configured, SonicWALL CDP Offsite Backup is as simple to use as the basic CDP backup.

Step 1 Login to the SonicWALL CDP Agent User Interface.

Step 2 Click the **Policies** tab.

Step 3 To backup files designated in a CDP Files and Folders object to the offsite appliance, click the Edit icon for the object, click on the desired folder in the **Backup Folders** list, and then select the **Offsite Backup** checkbox.

Step 4 To backup files designated in a Fileset backup object or Applications object to the offsite appliance, edit the Backup Task and select the **Send all files offsite** option in the **Offsite** drop-down list.

Step 5 Click **OK**.

Viewing Backed Up Files on the Offsite Appliance

You can view the files that are backed up offsite in one of the following ways:

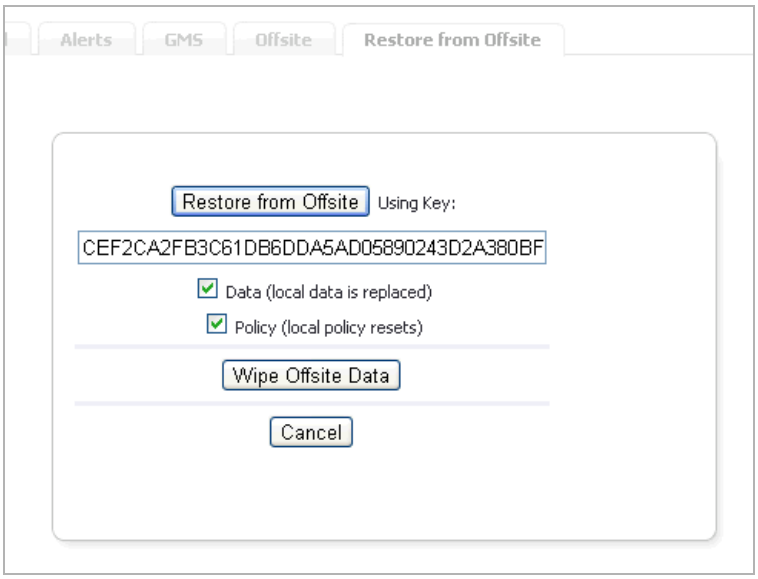
- Connect the SonicWALL CDP Agent User Interface to the downstream appliance, and use the Administrator File Browser to browse to the files and folders and applications that are backed up offsite. See “Using the Agent UI as Administrator” on page 96 for more information.
- In the Web Management Interface of the downstream appliance, navigate to the Agents > Browse Agent Files page and select Offsite. See “Browsing Agents Files” on page 92 for more information.

Recovering Data From the Upstream Appliance

To restore data and policy information from the upstream appliance to the downstream appliance, perform the following steps:

Step 1 Login to the downstream CDP appliance using the Web Management Interface.

Step 2 Navigate to the **System > Settings** page and click the **Restore from Offsite** tab.



Step 3 If a new downstream appliance is set up, verify that the correct key is in the key field.

Step 4 To restore data, select the **Data** checkbox.

Step 5 To restore settings and configurations, select the **Policy** checkbox.

Note Once the old appliance's settings and configurations are downloaded after selecting the **Policy** checkbox, the new appliance will begin backing up the local agents immediately. It may not be necessary to download the old data from the upstream appliance.

Step 6 Click **Restore from Offsite**.

Step 7 A warning message displays. Click **Yes** to continue.

Note The data on the downstream appliance will be replaced with the data from the upstream appliance.

Step 8 A second warning message displays. Click **Yes** to continue.

Note The data restore process cannot be canceled once it has started.

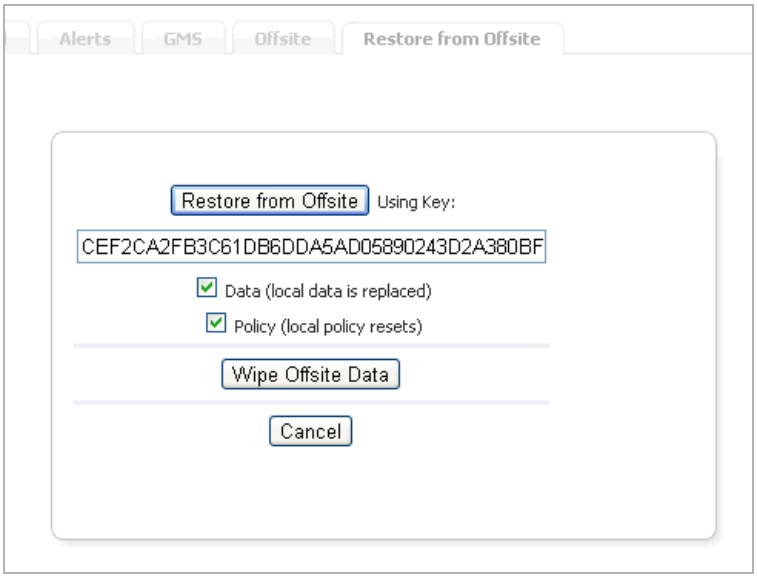
The restore progress displays. Click **Close** to close the progress page.

Deleting Data From the Upstream Appliance

To delete data and policy information from the upstream appliance, perform the following steps:

Step 1 Login to the downstream CDP appliance using the Web Management Interface.

Step 2 Navigate to the **System > Settings** page and click the **Restore from Offsite** tab.



Step 3 To delete data, select the **Data** checkbox.

Step 4 To delete settings and configurations, select the **Policy** checkbox.

Step 5 Click **Wipe Offsite Data**.

Step 6 A warning message displays. Click **Yes** to continue.

Replacing the Downstream CDP Appliance

If the downstream CDP is no longer accessible, a new CDP can take its place and recover data from the upstream appliance. The following information is required before you begin:

- Old CDP's registration code (to identify the original CDP)
- Old CDP's encryption key
- New CDP's registration code

To recover data from the upstream CDP appliance, you must first configure the upstream appliance to allow the new downstream appliance access to the old appliance's data. Then the new appliance must be setup to connect to the upstream CDP appliance.

Note The data on the downstream appliance will be replaced with the data from the upstream appliance. The data restore process cannot be canceled once it has started.

To update the upstream appliance with a different downstream appliance, perform the following steps:

Step 1 Login to the upstream CDP appliance using the Web Management Interface.

Step 2 Navigate to the **Agents > Manage** page.

Step 3 On the **Configure** tab, click the **Edit** icon for the old CDP that is being replaced.

Step 4 In the **Agent Name** and **Friendly Name** fields, replace the old CDP's IP address or FQDN with the new one and click **OK**.

You must now configure the new downstream appliance to backup to the upstream CDP appliance. Follow the directions in "Configuring the Downstream CDP Appliance" section on page 208 before recovering data from the upstream CDP appliance.

Disaster Recovery Using the Offsite Service

SonicWALL CDP Offsite Service allows the administrator to perform a disaster recovery when local data have been rendered unrecoverable. This means that the local SonicWALL CDP appliance is unusable and must be replaced. Data can be recovered from the Offsite Service in the event that a disaster renders local data corrupted, destroyed or otherwise unrecoverable.

Note Data cannot be recovered from the Offsite Service without the Encryption Key, even by SonicWALL technical support engineers. It is advised that you store your encryption key in a secure location, such as a safe or bank. Your encryption key may be viewed by selecting the **Offsite** tab on the System > Settings page of the Web Management Interface. For more information, refer to the "Configuring the Downstream CDP Appliance" section on page 208.

To recover data from the Offsite Service after the original local SonicWALL CDP appliance has become unusable, perform the following steps:

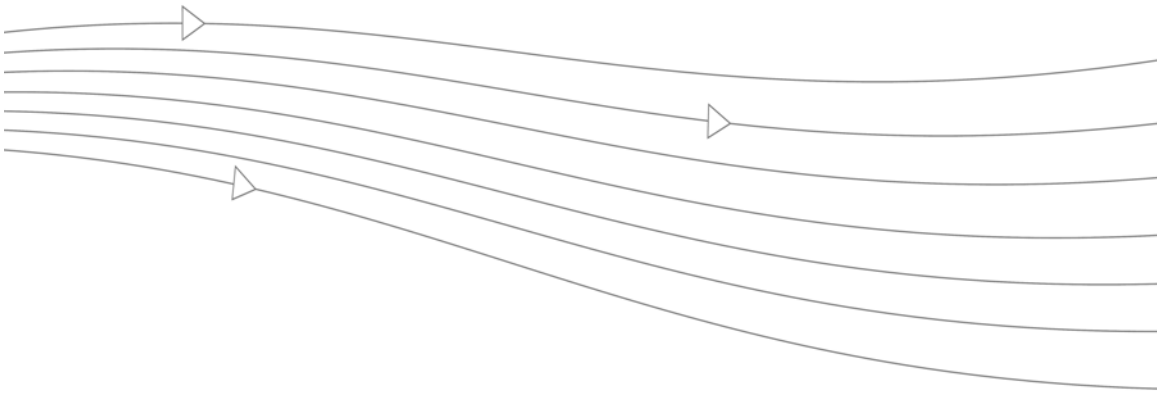
Step 1 Locate your encryption key, which should be stored in a safe location, such as a vault or bank.

Step 2 Verify that your SonicWALL CDP appliance is under warranty or extended warranty. If it is not under warranty, it will be necessary to purchase a replacement SonicWALL CDP appliance with enough storage to contain the data recovered from the Offsite Service. Contact your SonicWALL Technical Support representative for your replacement appliance.

Step 3 Configure the replacement SonicWALL CDP appliance to match the settings of the original appliance.

Step 4 Replace the encryption key of the replacement appliance with the encryption key of the original appliance.

Step 5 When the replacement appliance is properly configured with the encryption key from the original appliance, it will automatically recover data from the Offsite Service.



Chapter 13: Using Local Archiving

This chapter describes how to configure and use the Local Archive feature with your SonicWALL CDP appliance. This chapter includes the following sections:

- "SonicWALL CDP Local Archiving Overview" section on page 215
- "Creating a Local Archive" section on page 217
- "Restoring Client Data from a Local Archive" section on page 221
- "Restoring Server Applications from a Local Archive" section on page 223
- "Creating an Automatic Local Archive Task" section on page 226

SonicWALL CDP Local Archiving Overview

The Local Archiving feature and the Local Archiving Manager allow an administrator to copy some or all of the contents of the SonicWALL CDP appliance onto a USB device. This feature can also be used to create a portable backup that can be restored at another site that does not have a CDP appliance. Data can be archived to the USB device in encrypted format.

SonicWALL CDP Local Archiving provides the following benefits:

- Disaster-recovery—Local Archiving can be part of a flexible disaster-recovery program. Administrators can configure local archiving to run automatically, and use USB devices to replace tapes.
- Offsite storage—For some organizations, physical offsite storage is a regulatory requirement. Copying data to USB devices, which are then stored elsewhere, can fulfill regulatory requirements, especially when the data is securely encrypted.
- Upstream local archiving—You can create a local archive of data on an upstream (offsite) appliance, as well as on a local appliance. Having a local archive of data that has been backed up offsite adds flexibility and redundancy.
- Backup—In companies with multiple locations, the distributed branch offices can back up to a central location, which adds flexibility and redundancy.
- Security—Encrypted USB storage devices are more secure than many other methods of offsite storage.

How Does Local Archiving Work?

SonicWALL Local Archiving uses the Local Archive Manager application to backup files to a USB device, and to restore files from a USB device. The Local Archive Manager is automatically installed on your client during the initial SonicWALL CDP Agent installation process. By default, a shortcut is created for it on your desktop. Double-click the shortcut to launch the tool. If the shortcut is not available, you can launch the tool by double-clicking the **LocalArchiveAgent.exe** file in the SonicWALL CDP installation folder.

An administrator plugs a USB device into an upstream or downstream SonicWALL CDP appliance and then uses the SonicWALL CDP Local Archiving Manager to copy some or all of the contents of the CDP appliance to the USB device. The administrator specifies a source and destination, and whether the data should be archived in an encrypted format. The administrator then clicks **Archive Now!** to copy the data.

The administrator can also configure automated tasks to copy data from the SonicWALL CDP appliance to a USB device. By default, archived files are stored on the USB device as compressed, unencrypted files. Administrators can choose to add encryption to some or all of the archived files as they are stored on the USB device.

Local archives can be restored to Windows, Mac, or Linux agent machines.

Local Archiving Configuration Overview

The Local Archiving Manager provides the Appliance Archive button to activate local archiving. The feature allows an administrator to archive some or all of the contents of a SonicWALL CDP appliance onto a USB device. This feature can also be used to create a portable backup that can be restored at another site that does not have a SonicWALL CDP appliance. Data can be archived to the USB device in encrypted format.

The administrator can use local archiving manually or as part of an automated process. The configuration of source and destination folders is the same for both processes. For automated local archiving, the administrator must create one or more tasks.

To view the Appliance Archive window, click the **Appliance Archive** button in the Local Archiving Manager toolbar.

Local archiving is a licensed service offered at no additional charge. You must obtain a license on MySonicWALL before using this feature.

For more information about using this feature, see the “Creating a Local Archive” section on page 217.

Prerequisites for Local Archiving

Before configuring local archiving, make sure that the following requirements are met:

- The SonicWALL CDP Local Archiving Manager is configured and running properly.
- The local archiving module is properly licensed. The license is available on MySonicWALL at no additional charge.

- A USB device of sufficient capacity for your needs is plugged into the SonicWALL CDP appliance. SonicWALL recommends using NTFS on USB media. If you use FAT32, archiving is limited to files less than 4 gigabytes.

Note Local archiving requires a USB drive formatted for NTFS to archive files larger than 4 GB.

- If you plan to use your own encryption key to safeguard your data, the key should be available.

Creating a Local Archive

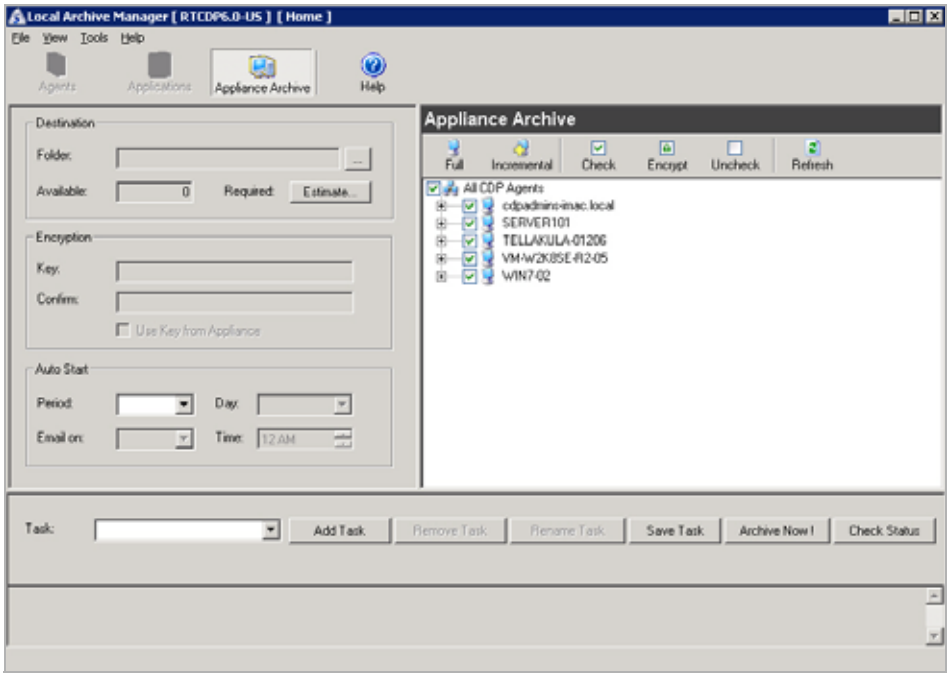
To set up a local archive, you must first choose a destination folder, and then the folder or folders you want stored on the USB device. These source folders exist on the SonicWALL CDP appliance. The administrator can also configure encryption for the folders. The administrator can set up recurring tasks that perform the local archiving on a regular schedule.

Note The time stamp of local archived files is in UTC time which may be different from the actual backup time in the local time zone.

To create a local archive on your USB device:

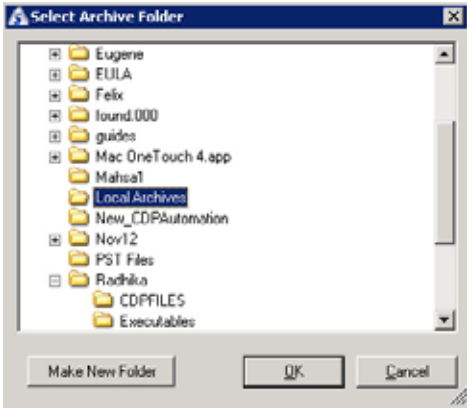
Step 1 Connect your USB device directly to the SonicWALL CDP appliance. You can connect it to a local appliance or to an upstream (offsite) appliance.

Step 2 Launch the SonicWALL CDP Local Archiving Manager and click **Appliance Archive** on the main toolbar.

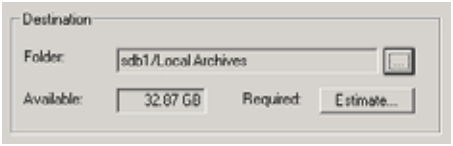


Step 3 Set the destination by clicking the **...** button next to the **Folder** field in the Destination section in the left pane. You'll see a list of all the USB devices mounted on your SonicWALL CDP appliance.

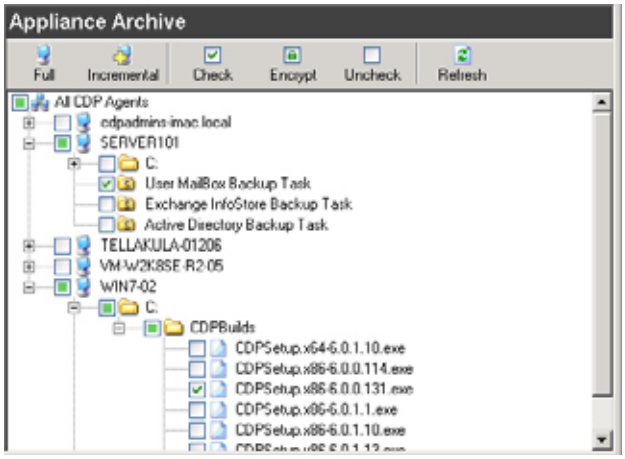
Step 4 Choose the USB device to which you want to copy your data. You can choose an existing folder on the USB device, or create a new one by clicking **Make New Folder**.



Step 5 Click **OK**. In the Destination section, you will see the folder you selected, and the space available on the USB device.



Step 6 In the Appliance Archive pane, choose the agent(s), applications, or folders you want to archive to the USB device. Select an entry by selecting the checkbox next to it.

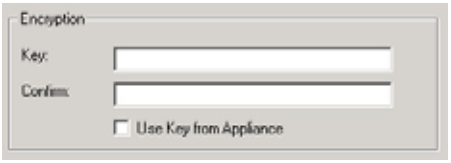


- If a node is marked with a check, all the files and folders below it will be included. If new files or folders are added to this node, they will automatically be added.
- To select only some folders, check only the folders you want. The levels above this partial folder are marked with a green block instead of a check mark. If a node is in partial mode, folders added to it will not automatically be added to the archived folders.

– To encrypt a folder as it is archived to the USB device, right-click its check box and choose **Encrypt**. By default, all the folders and files under an encrypted node will also be encrypted. When selected for encryption, the check box displays a lock icon instead of a check mark.

– To store an initial full version of a folder, and then only the changes thereafter, select the folders and then click **Incremental** at the top of the pane. The first time you archive this folder, all the files will be archived; the next time the local archiving runs, only the changed files will be archived.

Step 7 If you chose to encrypt any data, you must select an encryption key in the Encryption section in the left pane. Select the check box to use the encryption key stored on your SonicWALL CDP appliance. Otherwise, you can supply your own key, which can contain up to 32 alphanumeric characters.



Step 8 When you have configured local archiving, click **Archive Now!** Your data is archived to the USB device in the location you selected.

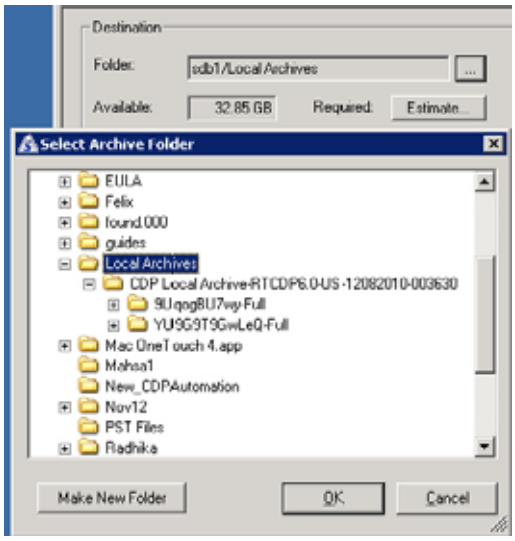
Step 9 You can stop the archiving at any time by clicking **Stop Archiving**. While the data is actively archiving, the **Archive Now!** button changes to **Stop Archiving**.

Note You can also use the button bar in the Local Archiving pane to configure an archiving task. All of the buttons except **Refresh** work like the menu options described above. Click **Refresh** to redraw the pane and be sure that you have the icons indicating the correct settings.

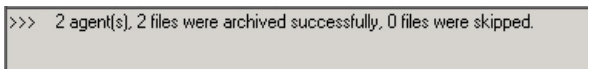
Caution You must eject the USB device before you unplug it. Failure to eject the device may cause data loss on the USB drive. See “Ejecting the USB Device” on page 220.

Verifying Local Archiving Success

To verify that your files have archived successfully, click **...** in the Destination section. Check that there are new folders in the location you selected, with the name of the appliance, current date, and time. Remember that the date and time are displayed in the UTC time zone.



At the bottom of the window, you will see a success message, detailing how many files were archived, and if there were any failures.



Caution You must eject the USB device before you unplug it. Failure to eject the device may cause data loss on the USB drive. See "Ejecting the USB Device" on page 220.

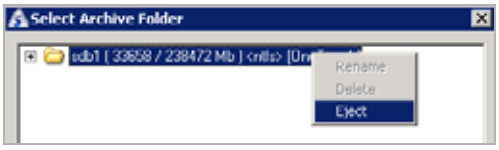
Ejecting the USB Device

To properly eject the USB device after archiving data to it, perform the following steps:

Step 1 In SonicWALL CDP Local Archiving Manager, click the **Appliance Archive** tab.

Step 2 In the left pane under Destination, click the **...** button next to the **Folder** field.

Step 3 In the Select Archive Folder window, right-click the USB drive entry and select **Eject**.



Step 4 In the confirmation dialog, click **Yes**.

Step 5 In the Select Archive Folder window, click **Cancel** to close the window.

Restoring Client Data from a Local Archive

To restore files, folders, or client applications (Outlook and Outlook Express) from a local archive on your USB device, open the SonicWALL CDP Local Archive Manager.

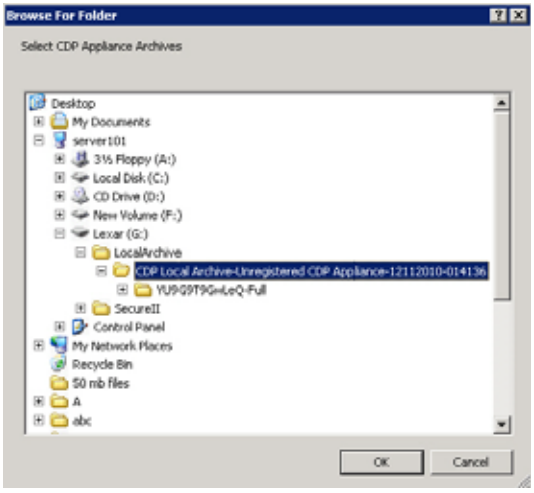
To restore server applications (Active Directory, Exchange InfoStore, SQL) from a local archive, follow the procedure described in "Restoring Server Applications from a Local Archive" on page 223.

To restore files, folders, or client applications from a local archive:

Step 1 Connect your USB device to the computer to which you want to restore the data. This might not be the same computer on which you run the SonicWALL CDP Local Archiving Manager.

Step 2 Launch the SonicWALL CDP Local Archiving Manager and click **Restore From Local Archive**. If Local Archiving Manager is already running, close it and then launch it again to view this selection. Note that you do *not* enter the password to login to an appliance when restoring from a local archive.

Step 3 In the Browse for Folder window, navigate to the USB drive and select the desired archive and then click **OK**. If the USB device contains multiple archives, they can be distinguished by the date in the file names.



Step 4 In the left pane, expand **Sets** and the folders under it to view the files available in the local archive. Select the item you want to restore.

Step 5 Click the **Restore a Version** button in the right pane.

Step 6 In the Restore Folder Version window, select the archive file to restore and then click **Restore**.

Step 7 In the Browse for Folder window, select a destination folder or click **Make New Folder** to create a folder for the restored data on your computer and then click **OK**.

Step 8 Wait until the restore completes. A dialog box displays the progress.

Restoring Server Applications from a Local Archive

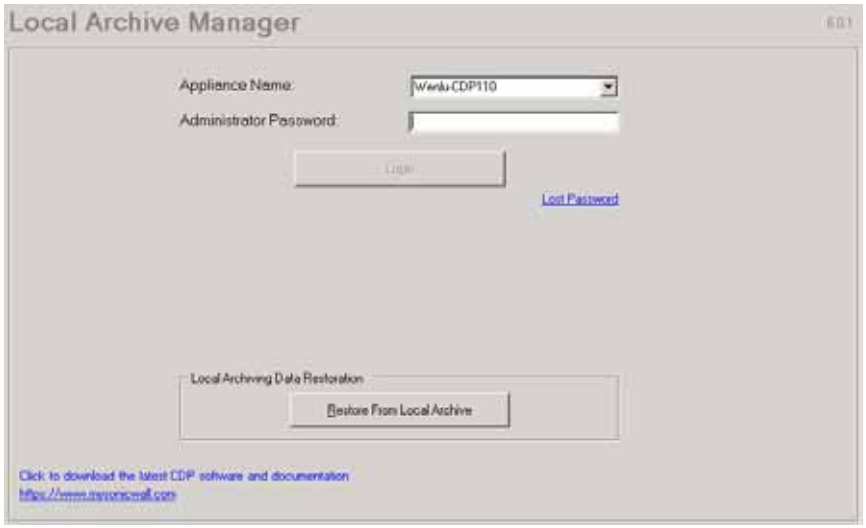
To restore server applications from a local archive, use the SonicWALL CDP Local Archiving Manager.

To restore files, folders, or client applications (Outlook and Outlook Express) from a local archive on your USB device, follow the procedure described in "Restoring Client Data from a Local Archive" on page 221.

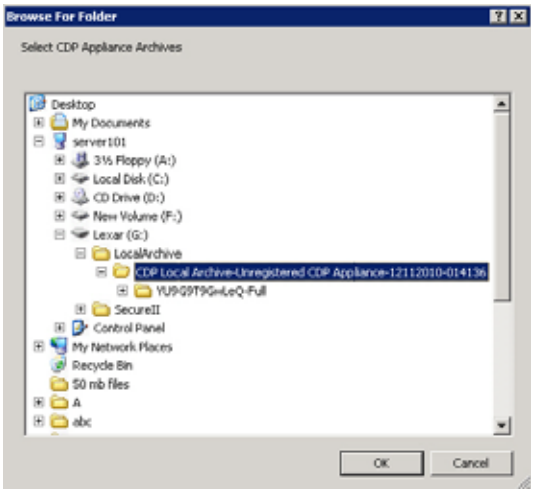
To restore server applications from a local archive, perform the following steps:

Step 1 Connect your USB device to the computer to which you want to restore the data. This might not be the same computer on which you run the SonicWALL CDP Local Archiving Manager.

Step 2 Launch the SonicWALL CDP Local Archiving Manager and click **Restore From Local Archive**. If Local Archiving Manager is already running, close it and then launch it again to view this selection. Note that you do *not* enter the password to login to an appliance when restoring from a local archive.

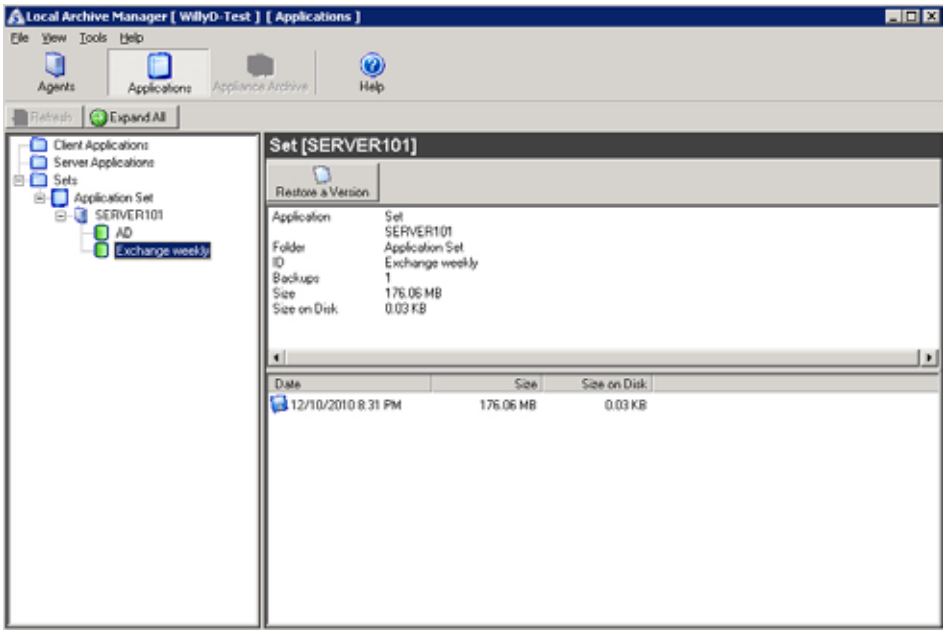


Step 3 In the Browse for Folder window, navigate to the USB drive, select the desired archive and then click **OK**. If the USB device contains multiple archives, they can be distinguished by the date in the file names.



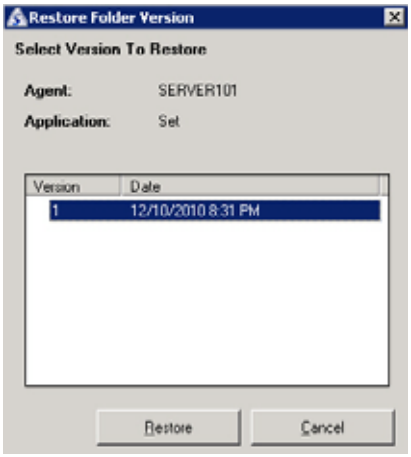
Step 4 In the Local Archiving Manager window, click **Applications** on the Local Archiving Manager toolbar.

Step 5 In the left pane, expand **Sets** and the folders under it to view the files available in the local archive. Select the item you want to restore.

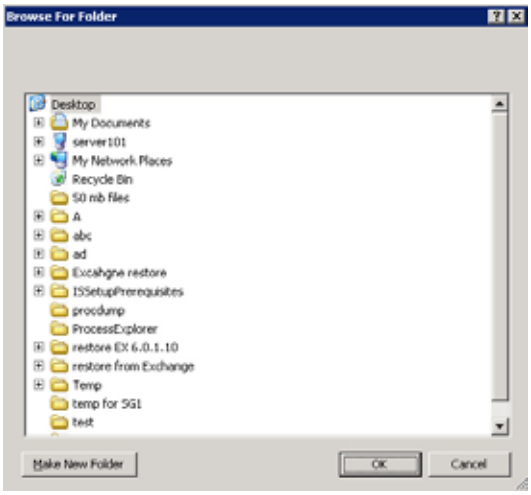


Step 6 Click the **Restore a Version** button in the right pane.

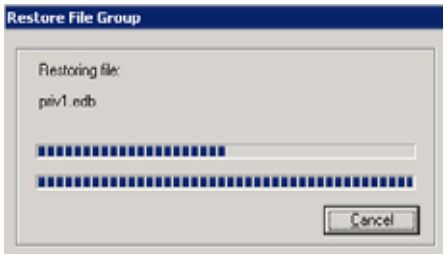
Step 7 In the Restore Folder Version window, select the archive file to restore and then click **Restore**.



Step 8 In the Browse for Folder window, select a destination folder or click **Make New Folder** to create a folder for the restored data on your computer and then click **OK**.



Step 9 Wait until the restore completes. A dialog box displays the progress.



Creating an Automatic Local Archive Task

You can configure the Local Archiving feature to automatically run at set intervals. Each task can run at only one interval, but you can set up multiple tasks on the same group of files. For instance, you could set up one task to run a full backup of a folder on Sunday, and then add a second task to do incremental backups the rest of the week. Tasks are stored on the CDP appliance.

Follow this procedure to manually configure Local Archiving:

Step 1 In the Auto Start section, choose a period (or interval) and time.

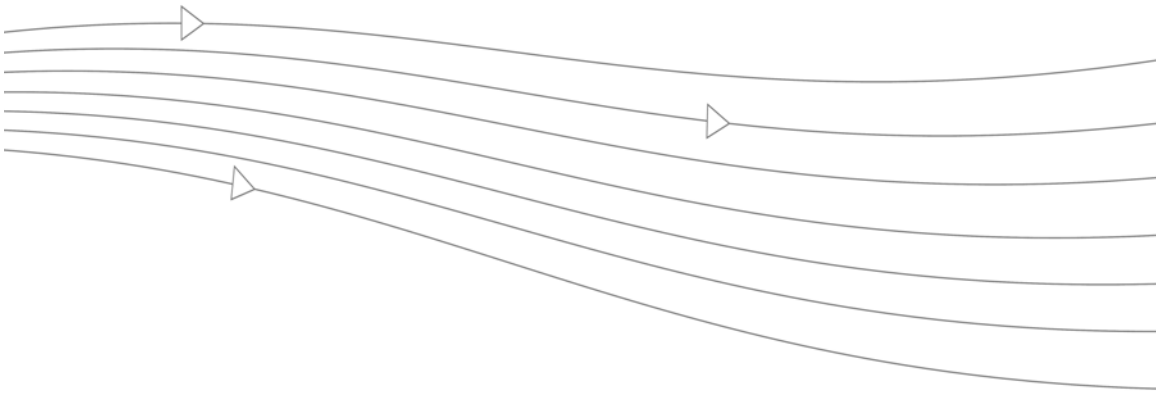
Step 2 If you want email notification (success or failure), specify when you want the message to be sent.

Step 3 In the **Task** field, enter the name for this task.

Step 4 Click **Save Task**.

Step 5 To add another task, click **Add Task** and configure it with a different period and time.

Step 6 To remove or rename a task, select it from the drop-down list, and then click the appropriate button.



Appendix

This appendix provides an overview of the online help feature, troubleshooting information, deployment guidelines for SonicOS, frequently asked questions, a command line reference, and a glossary.

See the following sections:

- “Help Overview” section on page 228
- “Troubleshooting SonicWALL CDP” section on page 228
- “Configuring SonicOS Security Services for SonicWALL CDP” section on page 232
- “Technical Frequently Asked Questions” section on page 235
- “Command Line Interface Reference” section on page 236
- “Glossary” section on page 248
- “Related Documents” section on page 250
- “Contributors” section on page 250

Help Overview

Help, a function within the Web Management Interface, redirects the administrator to online SonicWALL CDP help content.

To view the help content, click the **Help** button

in the Web Management Interface toolbar.

Troubleshooting SonicWALL CDP

This section contains troubleshooting information for the SonicWALL CDP. This section contains the following subsections:

- "Appliance Troubleshooting" section on page 228
- "Software Troubleshooting" section on page 228
- "Backup and Recovery Troubleshooting" section on page 229
- "Recovery when RAID Fails" section on page 232

Appliance Troubleshooting

This section contains troubleshooting that relates to the SonicWALL CDP appliance.

Symptom: Cannot connect to CDP Appliance

- Verify that your workstation/server has network level connectivity to the CDP appliance by attempting to ping the CDP appliance at its configured address.
- If you are on a separate subnet, you many enter the appliance IP address manually
  - Select **CDP Manual Connection**
  - Type in the CDP appliance IP address.
- Ensure that an agent firewall is not blocking the CDP Agent User Interface from connecting to the SonicWALL CDP appliance.

Enable firewall exceptions for Lasso.Client.exe, CDPAutoUpdate.exe and CDPAgent.exe.

Software Troubleshooting

This section contains troubleshooting that relates to the SonicWALL CDP software.

Symptom: Agent will not update

- Updates to the agent and appliance are downloaded and installed automatically in a process that is transparent to the user.
  - If there is no new update available during a manual update, no update will be made.
- Verify the current version of your product by navigating to the to the System tab in the SonicWALL CDP Agent User Interface.

Configuring SonicWALL CDP to Use a Public Server Instead of Windows Workgroups

Administrators using a Windows Workgroup may notice that their computer can access the network, but the CDP device cannot. This is because the CDP appliance is not compatible with Windows Workgroups.

Since certain networks demand that you join a Workgroup, the CDP administrator may not be able to upgrade the firmware.

As a solution, the administrator must configure the CDP device with a public server, rather than a private server.

To use a public server you need to configure the CDP Web management interface network settings. To do this, complete the following steps:

Step 1 On your Windows machine, navigate to **Network Connections**.

Step 2 Right-click **Local Area Connections**.

Step 3 Select **Properties**.

Step 4 Select **TCP/IP Properties**.

Step 5 Configure a Public IP, such as: 10.50.158.52.

Step 6 Click **OK** in each dialog box.

Symptom: Cannot open Web Management Interface

- Verify that CDP Agent User Interface is not running.

The Web Management Interface and the Agent User Interface cannot be open simultaneously on the same PC.

Backup and Recovery Troubleshooting

This section contains troubleshooting that relates to the SonicWALL CDP backup and recovery process. See the following:

- “Symptom: Initial backup seems slow” on page 230
- “Symptom: Files do not appear to be backing up” on page 230
- “Symptom: Applications are not available when adding a backup policy” on page 230
- “Symptom: A Permission Denied error is seen when restoring User Mailboxes” on page 231

Symptom: Initial backup seems slow

- Because SonicWALL CDP performs file compression and intelligent file management, the initial backup of files and folders may take some time depending on folder volume and size.
  - For example, if you are trying to backup 100,000 files averaging 200 KB, it could take up to 24 hours to complete.

Symptom: Files do not appear to be backing up

- Verify that SonicWALL CDP has access to the folders that you are trying to backup.
  - Verify that SonicWALL CDP Agent User Interface is started in the services tab.
  - By default, SonicWALL CDP uses the System account to access to the folders that are selected for backup.
  - The System account will need to be added to the security settings of any directory that you want to backup.

Symptom: Applications are not available when adding a backup policy

The SonicWALL CDP Agent uses a discovery process to find applications available for backup. The Volume Shadow Copy service and VSS Writer service must not be disabled for the discovery process to work.

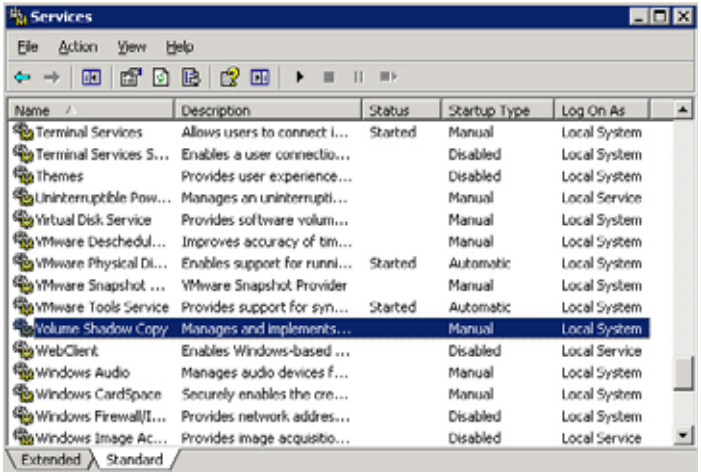
Volume Shadow Copy Service

To ensure that the SonicWALL CDP Agent can discover available applications, including Outlook, Outlook Express, System State and Active Directory, Exchange Infostore, Exchange User Mailbox, SQL Server, and Sharepoint, verify that the Volume Shadow Copy service is not disabled.

To view and configure the startup method for the Volume Shadow Copy service, perform the following steps:

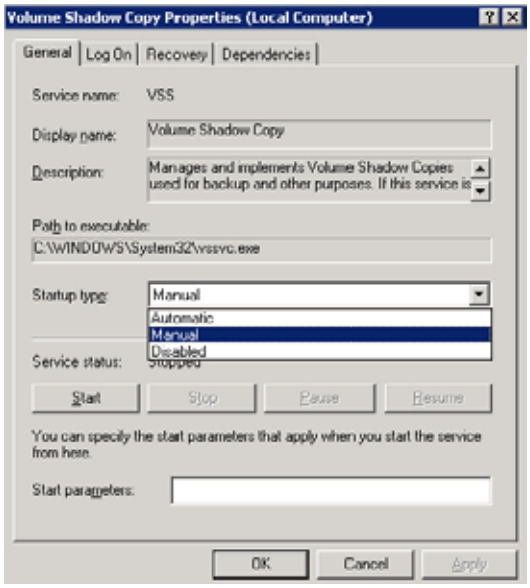
Step 1 Open the Windows Services window by selecting **Start > Administrative Tools > Services**.

Step 2 Scroll down to the Volume Shadow Copy service.


Services
File Action View Help
Name Description Status Startup Type Log On As
Terminal Services Allows users to connect i... Started Manual Local System
Terminal Services S... Enables a user connectio... Disabled Local System
Themes Provides user experience... Disabled Local System
Uninterruptible Pow... Manages an uninterrupti... Manual Local Service
Virtual Disk Service Provides software volum... Manual Local System
VMware Deschedul... Improves accuracy of tim... Manual Local System
VMware Physical Di... Enables support for runni... Started Automatic Local System
VMware Snapshot ... VMware Snapshot Provider Manual Local System
VMware Tools Service Provides support for syn... Started Automatic Local System
Volume Shadow Copy Manages and implements... Manual Local System
WebClient Enables Windows-based ... Disabled Local Service
Windows Audio Manages audio devices f... Manual Local System
Windows CardSpace Securely enables the cre... Manual Local System
Windows Firewall/I... Provides network addres... Disabled Local System
Windows Image Ac... Provides image acquisitio... Disabled Local Service
Extended Standard

Step 3 If it is **Disabled**, right-click it and select **Properties**.

Step 4 In the Volume Shadow Copy Properties window, select **Manual** from the **Startup type** drop-down list.



Step 5 Click **OK**.

VSS Writer Service

By default on Windows Server 2003 SBS, the VSS Writer service is disabled. To ensure that the SonicWALL CDP Agent can discover Microsoft Exchange and SQL applications, the VSS Writer service must be enabled.

To enable the VSS Writer service, perform the following steps:

Step 1 Select **Start > Run**, type **regedit**, and then click **OK**.

Step 2 In the Registry Editor, locate and then double-click the following registry subkey:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS\ParametersSystem
```

Step 3 Double-click the **Disable Exchange Writer** value.

Step 4 In the **Value** data text box, change the value from **1** to **0**, and then click **OK**.

Step 5 Quit the Registry Editor.

Step 6 Open the Windows Services window by selecting **Start > Administrative Tools > Services**.

Step 7 Stop and then restart the Microsoft Exchange Information Store service.

Symptom: A Permission Denied error is seen when restoring User Mailboxes

- Verify that you are logged in as “cdpadmin” to the system on which you are trying to restore the user mailboxes. Logging in as “Administrator” and then accessing the Exchange User Mailbox application with “cdpadmin” privileges does not work.

Recovery when RAID Fails

If you are using the SonicWALL CDP 5040 or 6080, or 3440i or 4440i appliances, your data will be protected by the additional failover protection of a RAID system in the event that a drive goes down.

SonicWALL CDP 3440i has RAID 1, which involves two disks, with data mirroring from one disk onto another.

SonicWALL CDP 5040 and 6080 and 4440i appliances have RAID 5, which involves three or more disks, with block-level data striping with distributed parity across the drive set.

This section contains the following subsections:

- "If One Disk Fails While Using the SonicWALL CDP 3440i" section on page 232
- "If Two Disks Fail While Using SonicWALL CDP 3440i" section on page 232
- "If One Disk Fails While Using SonicWALL CDP 5040 / 6080 / 4440i" section on page 232
- "If Two Disks Fail While Using SonicWALL CDP 5040 / 6080 / 4440i" section on page 232

If One Disk Fails While Using the SonicWALL CDP 3440i

If one disk fails while using the SonicWALL CDP 3440i:

- Contact SonicWALL Technical Support. Though your system will remain operational, it is necessary to correct the disk failure.

If Two Disks Fail While Using SonicWALL CDP 3440i

If two disks fail while using the SonicWALL CDP 3440i:

- Contact SonicWALL Technical Support. Your system will no longer be operational.

If One Disk Fails While Using SonicWALL CDP 5040 / 6080 / 4440i

If one disk fails while using the SonicWALL CDP 5040 or 6080 or 4440i:

- Contact SonicWALL Technical Support. Though your system will remain operational, it is necessary to correct the disk failure.

If Two Disks Fail While Using SonicWALL CDP 5040 / 6080 / 4440i

If two disks fail while using the SonicWALL CDP 5040 or 6080 or 4440i:

Contact SonicWALL Technical Support. Your system will no longer be operational.

Configuring SonicOS Security Services for SonicWALL CDP

When using SonicWALL CDP in conjunction with a SonicWALL firewall appliance, it is necessary to add the CDP appliance to the Security Services exclusion lists.

To configure the Security Services firewall exception list for CDP, perform the following tasks:

- "Clearing the Enforce Host Tag Search for CFS Setting" on page 233

- "Setting up Security Services for SonicWALL CDP" on page 233

Clearing the Enforce Host Tag Search for CFS Setting

To clear the Enforce Host Tag Search for CFS setting, perform the following steps:

Step 1 In your browser, navigate to the unlinked Diag page for the SonicWALL network security appliance, available at:
https://<firewall IP address>/diag.html

Step 2 In the left pane, click on the **Internal Settings** button.

Step 3 Under Security Services Settings in the right pane, clear the **Enforce Host Tag Search for CFS** checkbox.

Step 4 Click **Accept** at the top of the page.

Step 5 Click the **Close** button to return to the SonicOS management interface.

Setting up Security Services for SonicWALL CDP

This section describes the steps needed when adding a SonicWALL CDP appliance to your network when you are running SonicOS Security Services. To prevent the Security Services from blocking access to your SonicWALL CDP appliance, you must configure SonicOS Security Services with exclusions for the IP address of the appliance.

To configure SonicOS Security Services with exclusions for the SonicWALL CDP appliance, perform the following steps:

Step 1 Navigate to the **Security Services > Content Filter** page.

Step 2 Under **CFS Exclusion List**, select the **Enable CFS Exclusion List** checkbox.

Step 3 Click the **Add** button and add the SonicWALL CDP IP address to the list.

Step 4 Click **OK** in the Add dialog box, then click **Apply** on the Content Filter page.

Step 5 Navigate to the **Security Services > Client AV Enforcement** page.

Step 6 Under **Administration**, click **Configure**.

Step 7 In the **AV Config View** window, under **Client Anti-Virus Enforcement**, select the **Exclude specified address ranges from Client Anti-Virus enforcement** radio button.

Step 8 Click the **Add** button and add the SonicWALL CDP IP address to the list.

Step 9 Click **OK** in the Add dialog box and Config View window, then click **Apply** on the Client AV Enforcement page.

Step 10 Navigate to the **Security Services > Gateway Anti-Virus** page.

Step 11 Under **Gateway AV Settings**, select the **Enable HTTP Byte-Range requests with Gateway AV** checkbox.

Step 12 Under **Gateway Anti-Virus Global Settings**, click the **Configure Gateway AV Settings** button.

Step 13 In the **Gateway AV Config View** window, under **Gateway AV Exclusion List**, select the **Enable Gateway AV Exclusion List** checkbox.

Step 14 Click the **Add** button and add the SonicWALL CDP IP address to the list.

Step 15 Click **OK** in the Add dialog box and Config View window, then click **Apply** on the Gateway Anti-Virus page.

Step 16 Navigate to the **Security Services > Intrusion Prevention** page.

Step 17 Under **IPS Global Settings**, click the **Configure IPS Settings** button.

Step 18 In the **IPS Config View** window, under **IPS Exclusion List**, select the **Enable IPS Exclusion List** checkbox.

Step 19 Click the **Add** button and add the SonicWALL CDP IP address to the list.

Step 20 Click **OK** in the Add dialog box and Config View window, then click **Apply** on the Intrusion Prevention page.

Step 21 Navigate to the **Security Services > Anti-Spyware** page.

Step 22 Under **Anti-Spyware Global Settings**, click the **Configure Anti-Spyware Settings** button.

Step 23 In the **Anti-Spyware Config View** window, under **Anti-Spyware Exclusion List**, select the **Enable Anti-Spyware Exclusion List** checkbox.

Step 24 Click the **Add** button and add the SonicWALL CDP IP address to the list.

Step 25 Click **OK** in the Add dialog box and Config View window, then click **Apply** on the Anti-Spyware page.

Technical Frequently Asked Questions

This section contains a list of technical FAQs documented by SonicWALL technical support engineers to address common deployment questions. Table 1 lists the technical FAQs in this section.

Table 1 Technical FAQs

FAQ
"Q: How do I backup mapped drives?" section on page 235
"Q: How do I back up SQL database in mixed mode?" section on page 235

Q: How do I backup mapped drives?

A: SonicWALL CDP cannot backup mapped drives. Agent User Interface software must be installed on the computer where the data for backup resides. If you want to backup data stored on a server that has a mapped drive, you will still need to have the CDP Agent User Interface software installed and configured on the server.

Q: How do I back up SQL database in mixed mode?

A: To back up the SQL data base in mixed mode, the SQL server must be configured for mixed mode authentication. In addition, the SQL account must be part of SQL system administrators, and must have DBO access to the master database and all other application databases that are marked for backup. These settings can be configured using SQL Web Management Interface.

To configure the SQL server for mixed mode authentication, perform the following steps:

Step 1 Launch **SQL Server Web Management Interface**.

Step 2 Right click on the SQL server instance and choose **Properties**. This will launch the SQL server properties screen.

Step 3 Click the **Security** tab.

Step 4 Select SQL Server and Windows

To set the SQL account as part of SQL system administrators, perform the following steps:

Step 1 Expand **Security** tab under SQL server instance.

Step 2 Click on **Logins**.

Step 3 Highlight the SQL account on the right side of the screen and double click.

Step 4 Click the **Server Roles** tab.

Step 5 Select **System Administrators**.

To verify that the SQL account has DBO access to master database and all other application databases that are marked for backup, perform the following steps:

Step 1 Expand security tab under SQL server instance.

Step 2 Click on **Logins**.

Step 3 Highlight the SQL account on the right side of the screen and double click.

Step 4 Click the **Database** tab.

Step 5 Verify that the account has **db_owner** selected for all databases intended for backup.

Command Line Interface Reference

This section describes each SonicWALL CDP Command Line Interface (CLI) command. There are two types of commands: executables and system variables. Typing in a system variable by itself will return the current value of the variable. To update a variable, type it in followed with a proper value. Some executable commands take an argument, but most do not.

bmr

SNWLCLI> **bmr [{useradd <username> <passwd> <quota> | userdel <username> | passwdchange <username> <newpasswd> | quotachange <username> <newquota>}]**

With no arguments, displays list of Bare Metal Recovery accounts. With arguments, changes the list.

Arguments:

<*username*>: User account name to be added or deleted, or for which to change the password or quota

<*passwd*>: Password for an account being added

<*newpasswd*>: New password for an account being changed

<*quota*>: Quota for an account being added

<*newquota*>: New quota for an account being changed

Type: System Variable

Defaults: none

Related Commands: none

date

SNWLCLI> **date**

This variable controls the date on the appliance.

Arguments: none

Type: System Variable

Defaults: none

Related Commands: **time**

dig

SNWLCLI> **dig** [**@global-server**] [**domain**] [**q-type**] [**q-class**] {**q-opt**} {**global-d-opt**} **host** [**@local-server**] {**local-d-opt**} [**host** [**@local-server**] {**local-d-opt**}]

This is the standard **dig** command from the bind-tools package. Use this command to troubleshoot DNS related issues, such as:

- Connectivity to DNS server
- Outbound emails being queued
- DNS does not resolve into an IP address to connect

Arguments:

q-class: one of in,hs,ch

q-type: one of a,any,mx,ns,soa,hinfo,axfr,txt (Use ixfr=version for type ixfr)

q-opt is one of:

-x dot-notation: shortcut for in-addr lookups

-i: IP6.INT reverse IPv6 lookups

-f filename: batch mode

-b address[#port]: bind to source address/port

-p port: specify port number

-t type: specify query type

-c class: specify query class

-k keyfile: specify tsig key file

-y name key: specify named base64 tsig key

-4: use IPv4 query transport only

-6: use IPv6 query transport only

d-opt is of the form +keyword[=value], where keyword is:

+[no]vc: TCP mode

+[no]tcp: TCP mode, alternate syntax

+time=###: Set query timeout [5]

+tries=###: Set number of UDP attempts [3]

+retry=###: Set number of UDP retries [2]

+domain=###: Set default domainname

+bufsize=###: Set EDNS0 Max UDP packet size

+ndots=###: Set NDOTS value

+[no]search: Set whether to use searchlist

+[no]defname: Ditto

+[no]recurse: Recursive mode

+[no]ignore: Don't revert to TCP for TC responses

+[no]fail: Don't try next server on SERVFAIL

+[no]besteffort: Try to parse even illegal messages

+[no]aaonly: Set AA flag in query (+[no]aaflag)

+[no]adflag: Set AD flag in query

+[no]cdflag: Set CD flag in query

+[no]cl: Control display of class in records

+[no]cmd: Control display of command line

+[no]comments: Control display of comment lines

+[no]question: Control display of question

+[no]answer: Control display of answer

+[no]authority: Control display of authority

+[no]additional: Control display of additional

+[no]stats: Control display of statistics

+[no]short: Disable everything except shortform of answer

+[no]ttlid: Control display of ttls in records

+[no]all: Set or clear all display flags

+[no]qr: Print question before sending

+[no]nssearch: Search all authoritative nameservers

+[no]identify: ID responders in short answers

+[no]trace: Trace delegation down from root

+[no]dnssec: Request DNSSEC records

+[no]multiline: Print records in an expanded format

global d-opts and servers (before host name) affect all queries.

local d-opts and servers (after host name) affect only that lookup.

Type: Executable

Defaults:

q-class: in

q-type: a

dns

SNWLCLI> **dns** [**--nameserver** <*ip*>]... [**--search** <*domain*>]...

This variable controls the DNS configuration settings on an appliance. Called with no arguments it will return the current configuration.

Arguments:

<*ip*>: IP address to be assigned to the server

<*domain*>: Domain name to be searched for

Type: System Variable

Defaults: q-class

drives

SNWLCLI> **drives**

This function outputs a list of drives registered with the system. Three types of drives are:

- System: Default data storage with operating system installed on it
- Internal: Additional internal device
- Temporary: Temporary external device, such as a USB drive

Arguments: none

Type: System Variable

Defaults: none

Related Commands: **time**

exit

SNWLCLI> **exit**

This function will exit out of the CLI.

Arguments: none

Type: Executable

Defaults: none

fetchurl

SNWLCLI> **fetchurl** [**-q**] <*URL*>

This function sends an HTTP request and dumps it to standard output.

Arguments:

<*URL*>: The URL being requested.

-q: quiet

-S: dump header in addition to response body

Type: Executable

Defaults: none

get

SNWLCLI> **get** <*arg*> [*arg*]

This function will retrieve configuration parameters.

Arguments: [*arg*]: Valid arguments that can be retrieved: ntp, ntpservers, syslogservers, tz

Type: Executable

Defaults: none

gms

SNWLCLI> **gms** <*interval*> [<server>…]

This variable stores the interval time between SonicWALL GMS heartbeat messages. Heartbeat messages allow SonicWALL GMS to monitor the SonicWALL CDP appliance.

Arguments:

<*interval*>: time in seconds between SonicWALL GMS heartbeat messages, set to 0 to disable

<server>:

Type: System Variable

Defaults: none

help

SNWLCLI> **help** <*command*>

This function will print help messages describing available commands from the CLI. Calling it with no arguments will print out a list of available commands. It can take a command name as an argument and will print out more detailed explanation of the given command.

Arguments:

<*command*>: name of a valid CLI command

Type: Executable

Defaults: all available commands

hostname

SNWLCLI> **hostname <***fqdn***>**

This function will display or set current host name. Calling it with no argument will display the current hostname.

Arguments:

<*fqdn*>: fully qualified domain name

Type: Executable

Defaults: snwl.example.com

interface

SNWLCLI> **interface** <*ifname* <*ip* **/** *bits* **|** *ip netmask*>>

This variable controls the configuration of interfaces. With no arguments, it will return the configuration of all available interfaces. Passing it an interface name as an argument will return all data related to the given interface. Passing it an interface name and an IP address will overwrite the current configuration of the interface.

Arguments:

<*ifname*>: name of interface to be configured

<*ip*>: new IP address to be assigned to interface

<*bits*>: bit rate to be assigned to interface

<*netmask*>: netmask to be assigned to interface

Type: System Variable

Defaults: current configuration

Example:

SNWLCLI> interface eth0 192.168.168.169/24

SNWLCLI> interface eth0 192.168.168.169 255.255.255.0

Example Use Case: Authentication Reset

Problem: You have lost the password and IP address for your SonicWALL CDP appliance.

Solution: First, reset the password to the default, and then determine the IP address of the SonicWALL CDP appliance. Connect a USB keyboard and monitor to your SonicWALL CDP appliance and perform the following steps:

a. Reboot the SonicWALL CDP appliance, and interrupt the boot process by tapping the **ESC** key on the keyboard as the boot process progresses, until you are in the GRUB bootloader screen. You will see a variety of options. Select the **Authentication Reset** option.

Your SonicWALL CDP will appear to partially reboot, and will perform an additional full reboot once more. Your username/password is reset to **admin** and the generic password, **password**.

b. Use the keyboard and monitor to log into the appliance using the **admin** user name and the current CDP password.

The SNWLCLI> prompt is displayed.

c. Type the following command to determine the IP address of the appliance:

SNWLCLI> **interface eth0**

The output will look similar to the following example:

```
eth0: 192.168.181.10  255.255.0.0
Media: Auto-detected
```

where 192.168.181.10 is the current IP address and 255.255.0.0 is the current subnet mask for the SonicWALL CDP default network adaptor.

d. If that IP address is not routable in your network (for example, it was set incorrectly or with a typo during setup), you can change the IP address on a laptop or another computer to an IP address on the same (incorrect) subnet, allowing you to gain access to the SonicWALL CDP web management interface to change the CDP IP address. Be sure to reset your laptop IP address to its previous setting after updating the IP address on the SonicWALL CDP.

iostat

SNWLCLI> **iostat** [options...] [<*interval*>[<*count*>]]

This is the standard input/output statistics utility.

Arguments:

[options]: see manual for details

<interval>: see manual for details

<count>: see manual for details

Type: Executable

Defaults: none

ntp

SNWLCLI> **ntp** <**on**|**off**> [<**default servers** | <*server*> [<*server*>]...>]

This variable controls the NTP (Network Time Protocol) on an appliance. With no arguments, it will print out the current NTP configuration. In order to change NTP configuration, pass “on” or “off” as a first argument followed by a list of NTP servers to use. Use this command to synchronize the time with a NTP server.

Arguments:

<**on**>: Enables NTP using currently configured NTP servers

<**off**>: Turn off NTP

<**default servers**>: Enables NTP and resets list of servers to the built-in defaults

<*server*>: specifies a server to be set in NTP list

Type: System Variable

Defaults: Current configuration

ping

SNWLCLI> **ping** [**-c** *COUNT*] [**-s** *SIZE*] [**-q**] *host*

This function is the standard ping function. Use this control to test connectivity. It also tests the appliance’s DNS lookup values.

Arguments:

host: target of ping

-c COUNT: send only COUNT pings

-s SIZE: Send SIZE date bytes in packets

-q: quite mode, only displays output at start and when finished

Type: Executable

Defaults: Sent SIZE data bytes in packets = 56

quit

SNWLCLI> **quit**

Exits out of the CLI.

Arguments: none

Type: Executable

Defaults: none

raidadd

SNWLCLI> **raidadd**

This function adds a new drive to the RAID array.

Arguments: none

Type: Executable

Defaults: none

Related Commands: **raidinfo**, **raidrebuild**, **raidremove**, **raidstatus**, **raidverify**

raidinfo

SNWLCLI> **raidinfo**

This function outputs information about the RAID devices in the box.

Arguments: none

Type: Executable

Defaults: none

Related Commands: **raidadd**, **raidrebuild**, **raidremove**, **raidstatus**,**raidverify**

raidrebuild

SNWLCLI> **raidrebuild** <controller> <array> [**--drive** <drive>]

This function will rebuild a drive within the raid array. With no arguments, it will display the rebuild status and scheduled jobs. With <*controller*> and <*array*> arguments, it rebuilds the array using an optional specified drive or the first available spare drive. Scheduling rebuilding operations is recommended as rebuilding an array can take a long time. SonicWALL recommends allowing a full night for the rebuilding process.

Arguments:

<*controller*>, <*array*>: rebuilds using an optional specified drive or a first available spare

<*drive*>: drive used to rebuild the array

Type: Executable

Defaults: none

Related Commands: **raidadd**, **raidinfo, raidremove**, **raidstatus**,**raidverify**

Example Use Case:

Problem: A SonicWALL CDP appliance has a degraded RAID array and displays the following information:

```
SNWLCLI> raidinfo
Controller: 2
Manufacturer: 3ware
Model: 9650SE-4LPML
Serial: L222008A8110095
Firmware: FE9X 4.06.00.004
Driver: 2.26.08.004-2.6.23

Array   Status          Size                Type
-----   ------          ----                ----
0       DEGRADED    2249961567683     RAID-5

Port    Status          Size              Model                              Serial
----    ------          ----              -----                               ------
0       UNKNOWN     N/A             N/A                                 N/A
1       OK              750156374016    WDC WD7502ABYS-01A6B0   WD-
WMATW0008111
2       OK              750156374016    WDC WD7502ABYS-01A6B0   WD-
WMATW0015222
3       OK              750156374016    WDC WD7502ABYS-01A6B0   WD-
WMATW0008333


SNWLCLI> raidstatus
Controller    Array 0
----------      --------
2             DEGRADED
```

Solution: Rebuild the RAID drive in the array with valid arguments, by performing the following steps:

a. In the CLI, execute **raidremove 2 0**, where the controller number is 2 and the drive port is 0.

This command should not generate any verbose output.

b. Execute **raidinfo** to check the status.

The status of port 0 should change to NOT-PRESENT.

c. Remove the bad disk and insert a new disk.

d. Execute **raidadd**.

e. Run **raidinfo** to check the status.

In the status output under Array, you will see two entries: 0 and 1:

```
Array   Status          Size                Type
-----   ------          ----                ----
0       DEGRADED    2249961567683     RAID-5
1       OK              750147176759      SPARE
```

f. Execute **raidrebuild 2 0 –drive 0**, to rebuild array 0.

You will see the following or similar output:

```
Controller    Array 0
----------    --------
2             0%
```

g. Run **raidinfo** to check status after starting the rebuild.

The status of the array will show as REBUILDING.

raidremove

SNWLCLI> **raidremove** <controller>, <port>

This function removes a defective drive from the RAID array. It takes the name of the drive to be removed as an argument.

Note The **raidremove** command must be executed before the bad disk is removed. Otherwise, there will be an error output.

Arguments:

<controller>:

<port>: removes the specified port

Type: Executable

Defaults: none

Related Commands: **raidadd**, **raidinfo, raidrebuild**, **raidstatus**,**raidverify**

raidstatus

SNWLCLI> **raidstatus**

This function prints out information about the status of the RAID arrays.

Arguments: none

Type: Executable

Defaults: none

Related Commands: **raidadd**, **raidinfo, raidrebuild**, **raidremove**, **raidverify**

raidverify

SNWLCLI> **raidverify** [{--**start**|--**stop**} **c**<controller>.**a**<array>=<m:h:D|**now**>|--**remove** <job>]

This function will verify the RAID array. With no arguments, it will display the verification status and scheduled jobs. Scheduling verifying operations is recommended as they can take a long time. SonicWALL recommends allowing a full night for RAID verification.

Arguments:

<*m:h:D***>**: schedule is expressed as either "now" or m:h:D where m is the minute, h is the hour, and D is the day of week 0-6 where 0 is Sunday, and * in any field means "every time"

<*job*>: rebuild job to be removed

--**start**: schedules verification start

--**stop**: schedules verification stop

--**remove**: removes verification job

Type: Executable

Defaults: displays verification status and scheduled jobs

Related Commands: **raidadd**, **raidinfo, raidrebuild**, **raidrebuild**, **raidstatus**

reboot

SNWLCLI> **reboot**

This function will reboot the appliance.

Arguments: none

Type: Executable

Defaults: none

reset

SNWLCLI> **reset**

This function will reset the appliance to factory defaults.

Arguments: none

Type: Executable

Defaults: none

restart

SNWLCLI> **restart** <appservices | postgresql | stunnel | webui>

This function restarts running services. It takes a service name as an argument.

Arguments:

<service>: service to restart

Type: Executable

Defaults: none

Related Commands: **stop**, **restart**

route

SNWLCLI> **route** < **--add** <*target*> **--destination** <*destination*> | **--remove** <*index*>>

This function acts like a system variable. With no argument, it will display routes. It can add routes if provided with an interface name or a gateway IP, or remove an existing route. Use this command to troubleshoot routing problems.

Arguments:

<*target*>: an IP address, net as IP/CIDR, or 'default' to be added as a target to the new route

<*destination*>: an interface name or a gateway IP

<*index*>: index number of the route to be removed

Type: Executable

Defaults: Current routes

Example Use Case:

Problem: You want to replace the gateway IP for your network, and add a route for it.

Solution: Execute the following command, where the new gateway IP address is 10.10.100.1:

SNWLCLI> **route --add 0.0.0.0/0 --destination 10.10.100.1**

snmp

SNWLCLI> **snmp <on | off>**

This variable holds the SNMP status. The current value will be displayed if the command is used without an argument.

Arguments:

<on>: enables SNMP

<off>: disables SNMP

Type: System Variable

Defaults: Current configuration

sshd

SNWLCLI> **sshd <on | off>**

This variable holds the sshd status. The current value will be displayed if the command is used without the argument.

Arguments:

<on>: enables sshd

<off>: disables sshd

Type: System Variable

Defaults: on

start

SNWLCLI> **start <***appservices* | *postgresq* | *stunnel* | *webui* **>**

This function starts services. It takes a service name as an argument. The list of services is application-specific.

Arguments:

<*service*>: service to start

Type: Executable

Defaults: none

Related Commands: **stop**, **restart**

stop

SNWLCLI> **stop <***appservices* | *postgresq* | *stunnel* | *webui* **>**

This function stops running services. It takes a service name as an argument. The list of services is application-specific.

Arguments:

<*service*>: service to stop

Type: Executable

Defaults: none

Related Commands: **start**, **restart**

telnet

SNWLCLI> **telnet** <*host*> [<*port*>]

This functions just like the interactive network communication program with the same name. It takes a host and a port as arguments. Use this tool to establish connectivity issues with a SMTP server. It is also useful to check if outbound SMTP rules on a firewall are well configured

Arguments:

<*host*>: hostname of telnet target

<*port*>: port number

Type: Executable

Defaults: none

time

SNWLCLI> **time** [<*YYYY/MM/DD hh:mm*>][TZ <*timezone*>]

This function controls the date, time, and the time zone.

Arguments:

<*YYYY>:* year

<*MM>:* month

<DD>: day

<hh>: hours

<*mm*>: minutes

<*timezone*>: timezone

Type: System Variable

Defaults: Current configuration

tsr

SNWLCLI> **tsr**

This function outputs an internal system state report. It does not take any arguments.

Arguments: none

Type: Executable

Defaults: none

tzlist

SNWLCLI> **tzlist**

This function outputs a list of all available time zones.

Arguments: none

Type: Executable

Defaults: none

version

SNWLCLI> **version**

This function displays the firmware and application version.

Arguments: none

Type: Executable

Defaults: none

Glossary

Active Directory: A centralized directory service system produced by Microsoft that automates network management of user data, security and resources, and enables interoperation with other directories. Active Directory is designed especially for distributed networking environments.

Advanced Encryption Standard (AES): A recent U.S. government encryption standard designed as the replacement for the aging Data Encryption Standard (DES).

Agent: A server, laptop or PC to be backed up using SonicWALL CDP.

Agent Service: A SonicWALL CDP software installed automatically on agents with Agent User Interface software. Agent Service communicates with the SonicWALL CDP appliance.

Agent User Interface: A SonicWALL CDP software installed on agents. Agent User Interface is a user interface for users of SonicWALL CDP agents that allows data backup and recovery configuration, as administered by the SonicWALL CDP Web Management Interface.

Backup Task: A defined File Set and Schedule are combined into a Backup Task for execution. Without a Backup Task, no backups will occur.

CDP Backup Method: One method of configuring file and folder backups on agents. The CDP method corresponds to the method used in the SonicWALL CDP 5.1 and earlier releases. Files are backed up individually rather than as a File Set, with new revisions created continuously as changes occur, up to a set limit of revisions.

Data De-duplication: The process used by SonicWALL CDP to back up only the blocks of data that have changed since the last scheduled backup. Metadata is used to map the changes between different revisions so that any revision can be restored correctly.

Domain Name System/Service (DNS): An Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they're easier to remember. The internet however, is really based on IP addresses. Every time you use a domain, therefore, a DNS service must translate the name into the corresponding IP addresses.

Downstream CDP appliance: A local CDP appliance on your LAN.

Dynamic Host Configuration Protocol (DHCP): A Protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses.

Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address. Many Internet Service Providers (ISPs) use dynamic IP addressing for dial-up users.

Web Management Interface: A SonicWALL CDP software installed on the SonicWALL CDP administrator's computer.

File Allocation Table (FAT): A table that the operating system uses to locate files on a disk. Due to fragmentation a file may be divided into many sections that are scattered around the disk. The FAT keeps track of all the pieces.

FileSet Backup Method: One method of configuring file and folder backups on agents. The FileSet method is new in the SonicWALL CDP 6.0 release. Files are backed up as a set of files for best synchronization, with new revisions created according to a configured schedule. Data de-duplication is used to back up only the blocks of data that have changed between scheduled intervals. The defined File Set and Schedule are combined into a Backup Task for execution.

High Availability: The capability of a mission-critical device, such as a SonicWALL security gateway, to automatically failover to a backup device in the event of a hardware failure on the primary unit.

Hyper Text Transfer Protocol (HTTP): The underlying protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands.

IP address (Internet Protocol): An Identifier for a computer device on a TCP/IP network. Networks using the TCP/IP protocol route message based on the IP address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255. For example, 1.160.10.240 could be an IP address.

Local Area Network (LAN): A computer network that spans a relatively small area. Most LANs are confined to a single building or group of buildings. However, one LAN can be connected to other LANs over any distance using telephone lines and radio waves. A systems of LANs connected in this way is called a wide-area network (WAN).

Master Boot Record (MBR): A small program that is executed when a computer boots up. Typically, the MBR resides on the first sector of the hard disk. The program begins the boot process by looking up the partition table to determine which partition to use for booting. It then transfers program control to the boot sector of that partition, which continues the boot process.

Policy: A set of rules administered from the SonicWALL CDP Web Management Interface. Policies are assigned directly to agents and define backup rights, quota, and other SonicWALL CDP capabilities.

Quota: The maximum amount of data a SonicWALL CDP agent can back up to the SonicWALL CDP appliance. The quota can be managed according to the number of files, the size of data on the appliance disk, or the size of the files being backed up. The two sizes can differ due to the data de-duplication feature.

Redundant Array of Independent Disks (RAID): A failover method used to protect against data loss in the event of disk failure.

Static IP address: An IP address that is unique and unchanging. Unlike dynamic IP addresses, a static IP address remains the same when you make a new Internet connection.

Upstream CDP appliance: An offsite CDP appliance on your WAN that is used for secure backup and recovery.

User Datagram Protocol (UDP): A connectionless protocol that sends and receive datagrams over an internet protocol (IP) network.

Universal Serial Bus (USB): An external bus standard that supports data transfer rates of 12Mbps. A single USB port can be used to connect up to 127 peripheral devices, such as mice, modems, and keyboard. USB also supports Plug-and-Play installation and hot plugging.

Related Documents

This section contains related documentation specific to SonicWALL CDP solutions.

User Guides

All online documentation for SonicWALL user's guides is available on the SonicWALL Support Web site at: http://www.sonicwall.com/us/support.html.

- *SonicWALL CDP 6.0 Agent User Interface User's Guide*
- *SonicWALL CDP 210/220 Getting Started Guide*
- *SonicWALL CDP 5040B Getting Started Guide*
- *SonicWALL CDP 6080B Getting Started Guide*
- *SonicWALL CDP 110/210 Getting Started Guide*
- *SonicWALL CDP 5040 Getting Started Guide*
- *SonicWALL CDP 6080 Getting Started Guide*
- *SonicWALL CDP 1440i/2440i Getting Started Guide*
- *SonicWALL CDP 3440i/4440i Getting Started Guide*
- *SonicWALL CDP Microsoft Exchange User Mailbox Feature Module*
- *SonicWALL CDP Microsoft Exchange InfoStore Feature Module*
- *SonicWALL CDP Site-to-Site Feature Module*
- *SonicWALL CDP Local Archiving Feature Module*

Contributors

Susan Weigand has over seven years of network security documentation experience. Prior to becoming a SonicWALL Senior Technical Writer, she worked for over ten years as a UNIX developer, and spent three years as a QA engineer at Cisco Systems and Symantec. At Symantec, Susan authored the *Symantec Network Security 7100 Series Implementation Guide* and contributed to other endpoint security and network security documents. She has taken a turn as the lead author on every SonicWALL product line over the past four years, preparing both administrator and user guides. Susan has also authored over 20 technical guides on network security topics and secure remote access solutions, including application firewall and control, high availability solutions, packet capture, switching, layer 2 bypass, single sign-on, custom reporting, application backup and restore, and Citrix access solutions. Susan holds two B.A. degrees in Computer Science and History, both with honors, and a Certificate in Internet Programming from the University of California at Santa Cruz.

Jean-Marc Catalaa, SonicWALL Curriculum Developer, holds a B.S. in Electrical Engineering from San Jose State University. Jean-Marc has written numerous technical documents and developed curriculum based on topics including multi-processor architecture, networking and wireless communications. He has taught over 40 classes about wireless communication in English, Spanish, Portuguese and Italian, adjusting training style for worldwide audiences and emphasizing hands-on learning.

Patrick Lydon has over five years of experience as a SonicWALL Technical Writer. He has authored over 20 technical guides on UTM, secure remote access solutions, Virtual Access Points, wireless site surveying, and RF monitoring. Patrick has also received an *International Photography Award* for *Fine Art Portraiture*. Patrick holds a B.A. degree in Design Studies with concentration in Graphic Design from San Jose State University.

Angela Mendoza is a Technical Writer with SonicWALL. She has a B.A. in English Literature, with an emphasis in Creative Writing, and a minor in Music from San Jose State University. Angela has earned distinction with several *2008 Phelan Awards* in the genres of *Best Short Story* and *Best Metrical Poetry* from San Jose State University.

Dave Parry is SonicWALL's Director of Platform Usability. Dave is one of SonicWALL's lead feature developers and is also the keeper of nearly a decade of SonicWALL institutional knowledge. Dave has designed and deployed networks for more than 100 companies worldwide, including a number of SonicWALL's most advanced and complicated customer networks. He has authored over one hundred SonicOS technotes for the SonicWALL Knowledge Base. Dave has also been instrumental in network troubleshooting and design, interoperability testing, lab maintenance, and performance testing. Dave designed and maintains the SonicWALL Live Demo site: http://livedemo.sonicwall.com/

Khai Tran has more than ten years of experience in networking documentation and works in San Jose, California, as technical documentation manager for SonicWALL. He leads SonicWALL's technical documentation teams, which have received numerous 5-star reviews in 2008 from the industry's leading publications and reviewers. Khai was a lead author of *Cisco IOS NetFlow Services Integrated Solutions Guide,* and a contributing author to *Cisco IOS Switching Services Configuration Guide.* He has also authored enterprise and service provider network solution guides for Boeing Aerospace and Electronic Arts. He holds a B.A. degree in English Modern Literature from U.C. Santa Cruz, a certificate in Technical Communications, and a Bilingual Teaching Credential from San Jose State University.

Index

Numerics

1440i
- hardware description 26

2440i
- hardware description 27

3440i
- hardware description 28

4440i
- hardware description 29

A

Active Directory 156
- authoritative restore 195
- backing up 156
- redundant domain controllers 192
- restoring 192
- safe mode 191

Agent User Interface 2
- about 94
- administrative use of 96
- default controls 95

agents
- adding 88
- browsing files on 92
- deleting 90
- editing name 89
- selecting policy 91
- service 9
- system requirements 22

applications
- Active Directory restore 192
- InfoStore backup 133, 145
- InfoStore restore 179, 184
- User Mailbox 126, 139
- user mailbox 176, 181

authentication
- SQL 167, 169
- Windows 168

B

backup task
- creating for fileset 79

backups
- Active Directory 156
- Exchange 126, 139
- InfoStore 133, 145
- offsite 20
- System State 156
- User Mailbox 126, 139

Bare Metal Recovery 18
- configuring account 100

C

CDP
- 1440i 26
- 2440i 27
- 3440i 28
- 4440i 29
- agent service 2
- appliance 2, 9
- firmware software 6
- licenses 60
- platform comparison, Gen 2 25
- platform comparison, Gen 3 24
- platform comparison, Gen 4 23
- purging data 56
- resetting to defaults 59

D

data
- purging 56

database
- Active Directory 156
- SQL 235
  - mixed mode 235

defaults
- resetting to 59

diagnostics
- system 59

domain controller
- safe mode 191

drives
- mapped 235
- RAID 40
- USB 217

E

encryption
- key 35

errors
database locked 199
Exchange
InfoStore Backup 133, 145
restore Storage Group 179, 184
user mailbox 176, 181
User Mailbox backup 126, 139
Expansion pack 41

F
factory defaults 59
files and folders
backup policy 72
backup task 79
creating object 73
schedule for backup 75
FileSets
recovering 172, 189
firmware
purging data 56

G
global policy
for files and folder backup 82

H
handshake-password 90
hard drive
replacing 41

I
InfoStore
backup 133, 145
restore 179, 184

K
key 90
encryption 35

L
licensing
CDP appliance 60
Local Archiving 216
site-to-site 206
Local Archiving
automating 226
creating 217
ejecting USB drive 220
overview 215
prerequisites 216
restoring from 221, 223
timestamps 217
verifying 220

M
master boot record 18

N
network
deployment requirements 22
DNS 65–66
domain 64
gateway 65
host name 64
IP address 65
subnet 65
testing connectivity 66
trace routes 68
URL connectivity 69

O
offsite
configuring settings 52
service 2, 19
disaster recovery 213
SQL backup 166
offsite storage
local archiving 215

P
policy
agent 91
global 82
purging data 56

R
RAID
Expansion pack 41
replacing a hard drive 41
System RAID 40
recovering
Exchange 176
files and folders 172, 189
from offsite 213
from offsite appliance 174
site-to-site 210, 212
SQL 196

Storage Group 179, 184
System State / Active Directory 191
User Mailbox 176, 181
recovery
Bare Metal 18
removing
downstream CDP in site-to-site 209
reporting
overview 107
restore
authoritative 195
Exchange 176
Files and Folders 172
from offsite appliance 174
SharePoint 189
SQL 196
Storage Group 179, 184
System State / Active Directory 191
restore to disk
Exchange, from Web UI 176

S

safe mode 191
schedule
for application backup 124
for files and folders backup 75
how scheduling works 16
security
AES 35
security key 90
server
system requirements 22
site-to-site
licensing 206
recovering data 210, 212
sample use cases 203
selecting files 210
SQL 235
account 166
authentication 167, 169
backing up 161
configuration levels 166
offsite backup 166
recovering with Agent UI 196
System State
backing up 156
components 157

T

technical support
International contact information v
North America contact information v
website v
trimming algorithms 81

U

USB
ejecting 220
for local archiving 217
User Mailbox
backup and restore application 126, 139
restoring 176, 181

W

Web Management Interface
purging data 56
reporting overview 107
system diagnostics 59
system licenses 60
system reset to defaults 59
Windows
authentication 168
supported versions 22

SonicWALL, Inc.

2001 Logic Drive
San Jose, CA 95124-3452

T +1 408.745.9600
F +1 408.745.9300

www.sonicwall.com

PN: 232-002020-00 Rev A

©2010 SonicWALL, Inc. is a registered trademark of SonicWALL, Inc. Other product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. Specifications and descriptions subject to change without notice.